UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

FACULTAD DE CIENCIAS ADMINISTRATIVAS

UNIDAD DE POSTGRADO

Gestión de seguridad de la información y los servicios críticos de las universidades:

un estudio de tres casos en Lima Metropolitana

TESIS

para optar el grado académico de Magíster en Administración con Mención en Gestión Empresarial

AUTOR

Rubén Alejandro Rayme Serrano

Lima-Perú

2007

A mis padres Hernán y Flora, por su esfuerzo en educarme y por su plena confianza, a mi esposa Patricia y a mi hija Alexandra, razón para seguir superándome personal y profesionalmente

A mis asesores por su apoyo invalorable y constante para la elaboración del presente trabajo.

INDICE

Pág.

Portada..... i
Dedicatoria..... ii
Índice..... iii
Índice de Cuadros……..... vi
Índice de Gráficos……..... viii
Resumen..... x
Abstract..... xii
INTRODUCCION..... 1

CAPITULO I
DISEÑO METODOLOGICO

1.1 PLANTEAMIENTO DEL PROBLEMA……..... 3
1.2 FORMULACION DEL PROBLEMA……..... 5
1.2.1 Problema principal……..... 5
1.2.2 Problemas específicos……..... 5
1.3 OBJETIVOS DE LA INVESTIGACION..... 5
1.3.1 Objetivo General..... 5
1.3.2 Objetivo específicos……..... 6
1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN..... 6
1.5 DELIMITACION DE LA INVESTIGACIÓN..... 7
1.6 HIPOTESIS DE LA INVESTIGACION……..... 8
1.6.1 Hipótesis General……..... 8
1.6.2 Hipótesis Auxiliares..... 8
1.7 VARIABLES DE LA INVESTIGACION……..... 8
Variable Independiente……..... 8
Variable Dependiente……..... 9
1.8 OPERACIÓN DE LAS VARIABLES……..... 9
1.9 ASPECTOS METODOLOGICOS……..... 10
1.9.1 Tipo de nivel de la investigación……..... 10
1.9.2 Población y Muestra……..... 11
1.9.3 Diseño de la Investigación……..... 12
1.9.4 Técnicas e Instrumentos de recolección de Datos……..... 12
1.9.5 Tratamiento y Procesamiento de los datos……..... 12

CAPITULO II
MARCO TEORICO

2.1 ANTECEDENTES DE LA INVESTIGACION……..... 13
2.2 BASES TEORICAS……..... 16
2.2.1 La Administración……..... 16
2.2.2 La Gestión de Seguridad de la Información……..... 19
2.2.2.1 La seguridad……..... 20
2.2.2.2 La información……..... 21
2.2.2.3 La seguridad de la información……..... 22
2.2.2.3.1 Necesidad de la seguridad de la información……..... 24

2.2.2.3.2 Requisitos de seguridad…… 25
2.2.2.3.3 Seguridad de los sistemas de información…… 30
2.2.3 Los Servicios de las Universidades..…….. 38
2.2.3.1 Servicios Críticos de las Universidades..…… 39

CAPITULO III
LA ENCUESTA Y ANALISIS DE RESULTADOS

3.1 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS……..... 43
3.1.1 Universidad Nacional Mayor de San Marcos……... 43
3.1.2 Universidad Nacional Federico Villarreal…….. 58
3.1.3 Universidad Privada San Juan Bautista ……... 73
3.2 PRUEBA DE HIPÓTESIS…….. 87
Hipótesis Auxiliar Nº 1 ……... 87
Hipótesis Auxiliar Nº 2…… 88
Hipótesis Auxiliar Nº 3…… 90
Hipótesis Auxiliar Nº 4…… 91

CAPITULO IV
PROPUESTA DE UN PLAN DE SEGURIDAD DE LA INFORMACION PARA LAS UNIVERSIDADES

4.1 SITUACIÓN ACTUAL…… 93
4.2 OBJETIVOS…… 97
4.3 EVALUACION DE RIESGOS Y ESTRATEGIAS DE SEGURIDAD……... 97
4.4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN…… 99
4.4.1 Organización de la Seguridad…… 100
4.4.2 Inventario de activos…… 100
4.4.3 Clasificación de la Información……... 101
4.4.4 Seguridad del Personal…… 102
4.4.5 Control de Acceso a los Datos…… 103
4.4.6 Gestión de Comunicaciones y Operaciones…… 106
4.4.7 Desarrollo y Mantenimiento de los Sistemas…….. 109
4.4.8 Cumplimiento Normativo…… 109
4.4.9 Gestión de Continuidad del Negocio…… 110
4.5 IMPLEMENTACION……... 111
4.5.1 Clasificación de la Información……... 111
4.5.2 Campaña de concienciación de usuarios…… 112
4.5.3 Seguridad de redes y comunicaciones…… 112
4.5.4 Inventario de acceso a los sistemas…… 113
4.5.5 Adaptación de contratos con proveedores……... 114
4.5.6 Verificación y adaptación de los sistemas a la Universidad…….. 114
4.5.7 Revisión y adaptación de procedimientos complementarios…… 115
4.6 CRONOGRAMA…….. 116
4.7 EVALUACION DE LAS ESTRATEGIAS DE SEGURIDAD…… 117

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES……..... 119
5.2 RECOMENDACIONES…….. 121

BIBLIOGRAFIA..... 123

ANEXOS…… 126
Anexo Nº 1 Encuesta de opinión a expertos en Tecnología de Información y Comunicaciones…… 126
Anexo Nº 2 Resolución Ministerial. PCM – Oficina Nacional de Gobierno Electrónico e Informática…… 129
Anexo Nº 3 ISO 27001: Sistema de Gestión de Seguridad de la información…… 131
Anexo Nº 4 Glosario de términos…… 135

INDICE DE CUADROS

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

Cuadro 01: ¿En la Universidad donde labora tiene políticas de seguridad de la Información?..... 43
Cuadro 02: ¿Si en la Pregunta 1 respondió si. Se cumplen o se llevan a la práctica estas políticas?..... 44
Cuadro 03: ¿Elija que beneficios se presentan cuando la Universidad cuenta con Políticas de Seguridad de la información?. Marcar una o más opciones 45
Cuadro 04: ¿Cuáles de estas medidas son las mas prioritarias en la Gestión de Seguridad de la información?.Marcar una más opciones…….. 46
Cuadro 05: ¿Cuáles son los errores más comunes cuando usa Internet y el correo electrónico?.Marcar una o más opciones…….. 47
Cuadro 06: ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?..... 48
Cuadro 07: ¿Sus equipos de computo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?..... 51
Cuadro 08: ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?..... 52
Cuadro 09: ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?..... 53
Cuadro 10: ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?..... 54
Cuadro 11: ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad. Por qué?..... 55
Cuadro 12: ¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son matrícula de alumnos, admisión y registros, tesorería y trámites documentarios?..... 56
Cuadro 13: ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?..... 57

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL

Cuadro 14: ¿En la Universidad donde labora tiene políticas de seguridad de la Información?..... 58
Cuadro 15: ¿Si en la Pregunta 1 respondió si. Se cumplen o se llevan a la práctica estas políticas?..... 59
Cuadro 16: ¿Elija que beneficios se presentan cuando la Universidad cuenta con Políticas de Seguridad de la información?. Marcar una o más opciones 60
Cuadro 17: ¿Cuáles de estas medidas son las mas prioritarias en la Gestión de Seguridad de la información?.Marcar una más opciones…….. 61
Cuadro 18: ¿Cuáles son los errores más comunes cuando usa Internet y el correo electrónico?.Marcar una o más opciones…….. 62
Cuadro 19: ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?..... 63
Cuadro 20: ¿Sus equipos de computo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?..... 66
Cuadro 21: ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?..... 67
Cuadro 22: ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?..... 68

Cuadro 23: ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?..... 69
Cuadro 24: ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad. Por qué?..... 70
Cuadro 25: ¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son matrícula de alumnos, admisión y registros, tesorería y trámites documentarios?..... 71
Cuadro 26: ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?..... 72

UNIVERSIDAD PRIVADA SAN JUAN BAUTISTA

Cuadro 27: ¿En la Universidad donde labora tiene políticas de seguridad de la Información?..... 73
Cuadro 28: ¿Elija que beneficios se presentan cuando la Universidad cuenta con Políticas de Seguridad de la información?. Marcar una o más opciones 74
Cuadro 29: ¿Cuáles de estas medidas son las mas prioritarias en la Gestión de Seguridad de la información?.Marcar una más opciones…… 75
Cuadro 30: ¿Cuáles son los errores más comunes cuando usa Internet y el correo electrónico?.Marcar una o más opciones…… 76
Cuadro 31: ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?..... 77
Cuadro 32: ¿Sus equipos de computo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?..... 80
Cuadro 33: ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?..... 81
Cuadro 34: ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?..... 82
Cuadro 35: ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?..... 83
Cuadro 36: ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad. Por qué?..... 84
Cuadro 37: ¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son matrícula de alumnos, admisión y registros, tesorería y trámites documentarios?..... 85
Cuadro 38: ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?..... 86

PRUEBA DE HIPÓTESIS

Cuadro 39: Hipótesis Auxiliar Nº 1. …….. 87
Cuadro 40: Hipótesis Auxiliar Nº 2…… 89
Cuadro 41: Hipótesis Auxiliar Nº 3…… 90
Cuadro 42: Hipótesis Auxiliar Nº 4…… 92

SITUACION ACTUAL

Cuadro 43: Políticas de seguridad…….. 93
Cuadro 44: Protección de los equipos…….. 94
Cuadro 45: Capacitación…….. 94
Cuadro 46: Incidencias de seguridad…… 95

Cuadro 47: Riesgos más frecuentes…….. 96
Cuadro 48: Redes informáticas universitarias……..... 96

INDICE DE GRAFICOS

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

Gráfico 01: ¿La Universidad donde labora tienen políticas de seguridad de la Información?…… 43
Gráfico 02: ¿Si en pregunta 1 respondió si. Se cumplen o se llevan la la práctica estas políticas?..... 44
Gráfico 03: ¿Elija que beneficios se presentan cuando la Universidad cuenta con políticas de Seguridad de la información?.Marcar una o más opciones 45
Gráfico 04: ¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la Información?.Marcar una o más opciones…….. 46
Gráfico 05: ¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico?.Marcar una o más opciones……..... 47
Gráfico 06: ¿Cuáles son los riesgos y la frecuencia que se presentan en los Recursos de información?..... 48
06.1 Riesgos muy frecuentes …….. 48
06.2 Riesgos regularmente frecuentes …….. 49
06.3 Riesgos poco frecuentes…….. 50
Gráfico 07: ¿Sus equipos de cómputo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?..... 51
Gráfico 08: ¿Cuáles son las incidencias que se dan con más frecuencia por parte los usuarios que manejan información?..... 52
Gráfico 09: ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?..... 53
Gráfico 10: ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la Información?..... 54
Gráfico 11: ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad.¿Por qué?..... 55
Gráfico 12: ¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios?..... 56
Gráfico 13: ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la información en la gestión integral de la Universidad?..... 57

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL

Gráfico 14: ¿La Universidad donde labora tienen políticas de seguridad de la Información?…… 58
Gráfico 15: ¿Si en pregunta 1 respondió si. Se cumplen o se llevan la la práctica estas políticas?..... 59
Gráfico 16: ¿Elija que beneficios se presentan cuando la Universidad cuenta con políticas de Seguridad de la información?.Marcar una o más opciones 60
Gráfico 17: ¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la Información?.Marcar una o más opciones…….. 61
Gráfico 18: ¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico?.Marcar una o más opciones……..... 62
Gráfico 19: ¿Cuáles son los riesgos y la frecuencia que se presentan en los Recursos de información?..... 63

19.1 Riesgos muy frecuentes …….. 63
19.2 Riesgos regularmente frecuentes …….. 64
19.3 Riesgos poco frecuentes…….. 65
Gráfico 20: ¿Sus equipos de cómputo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?..... 66
Gráfico 21: ¿Cuáles son las incidencias que se dan con más frecuencia por parte los usuarios que manejan información?..... 67
Gráfico 22: ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?..... 68
Gráfico 23: ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la Información?..... 69
Gráfico 24: ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad.¿Por qué?..... 70
Gráfico 25: ¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios?..... 71
Gráfico 26: ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la información en la gestión integral de la Universidad?..... 72

UNIVERSIDAD PRIVADA SAN JUAN BAUTISTA

Gráfico 27: ¿La Universidad donde labora tienen políticas de seguridad de la Información?…… 73
Gráfico 28: ¿Elija que beneficios se presentan cuando la Universidad cuenta con políticas de Seguridad de la información?.Marcar una o más opciones 74
Gráfico 29: ¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la Información?.Marcar una o más opciones…….. 75
Gráfico 30: ¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico?.Marcar una o más opciones……..... 76
Gráfico 31: ¿Cuáles son los riesgos y la frecuencia que se presentan en los Recursos de información?..... 77
31.1 Riesgos muy frecuentes …….. 77
31.2 Riesgos regularmente frecuentes …….. 78
31.3 Riesgos poco frecuentes…….. 79
Gráfico 32: ¿Sus equipos de cómputo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?..... 80
Gráfico 33: ¿Cuáles son las incidencias que se dan con más frecuencia por parte los usuarios que manejan información?..... 81
Gráfico 34: ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?..... 82
Gráfico 35: ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la Información?..... 83
Gráfico 36: ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad.¿Por qué?..... 84
Gráfico 37: ¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios?..... 85
Gráfico 38: ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la información en la gestión integral de la Universidad?..... 86

RESUMEN

Existe una actitud histórica en la educación superior según la cual no debe haber restricciones para el acceso a la información; es en ese sentido que los docentes, alumnos, investigadores y terceros solicitan el acceso abierto a los sistemas de información de las Universidades. Sin embargo a la luz de las recientes amenazas de la información tales como: sabotajes, violación de la privacidad, intrusos, interrupción de servicios, etc. y de las expectativas de mayores amenazas a la seguridad en el futuro, no puede continuar este acceso abierto e ilimitado.

Por esta razón se realizó un estudio en tres Universidades de Lima Metropolitana: la Universidad Nacional Mayor de San Marcos (UNMSM), la Universidad Nacional Federico Villarreal (UNFV) y la Universidad Privada San Juan Bautista (UPSJB), teniendo como objetivo proponer estrategias de Gestión de Seguridad de la Información y sus implicancias en la calidad y eficacia en los servicios críticos de las universidades.

Cabe señalar que la muestra de la población estuvo conformada por 30 expertos del área de Tecnología de Información y Comunicaciones (TIC) que laboran en las 3 universidades citadas, a quienes se les aplicó un formulario de encuesta para medir sus opiniones con respecto a la gestión de seguridad y los servicios críticos.

Los resultados de la investigación revelaron las estrategias que se deben utilizar en la gestión de seguridad de la información como son: primero, la importancia de desarrollar políticas de seguridad: UNMSM 37 %, UNFV 19% y UPSJB 24%; segundo, los programas de capacitación al personal, donde los expertos consultados informaron el interés por asistir : UNMSM 60%, UNFV 70% y UPSJB 70% y tercero, la protección a los recursos de información, porque el 38% de los expertos manifestaron que sus centros informáticos no poseen equipos de protección contra cortes de energía eléctrica, amenaza que fue común en la década de 1980 -1990.

Los resultados también demostraron que al implementarse estas estrategias el impacto en las aplicaciones de red e internet será eficaz y de acuerdo a los expertos consultados se obtendrán beneficios tales como: una mejor protección de la información (50%) y una mejora de la calidad en el servicio a los alumnos y docentes (27%). Además se minimizarán los riesgos de la información, pues en el caso de la UNMSM la infección de virus informáticos es de 56%, mayor al de las otras universidades consultadas.

Con respecto a las incidencias de seguridad como son: la modificación desautorizada, divulgación ilícita y robo de la información, los resultados corroboraron lo que está pasando a nivel mundial donde el 70% de ellas son causados por los trabajadores, producto de errores, descuidos en sus conocimientos sobre la seguridad o por actos delictivos propiamente dichos.

Por otro lado, debemos recomendar a las autoridades universitarias desarrollar políticas de seguridad de la información o si las tienen hacerlas cumplir porque constituyen la base de un plan de seguridad. De la misma forma, es conveniente un programa educativo de toma de conciencia de seguridad relacionado con la capacitación de los trabajadores. También es necesario reestructurar las redes informáticas aplicando tecnología de prevención y detección de intrusos y separando el área académica con la administrativa pues ambos poseen servicios críticos.

Finalmente, se recomienda una propuesta piloto de un plan de seguridad de la información para las Universidades, que servirá para que éstas puedan tomarla como referencia para la implantación de sus propios planes de seguridad.

ABSTRACT

There has been historical attitude in the high education according to which there must not be restrictions for the access to information. So the teachers, students, researches and other people require an open access to the university information systems. Nevertheless, due to the last threats of the information such as sabotages, violation of privacy, intruders, service interruptions and some others, and opened to the forward major threats to security, this access can not continue being opened and unlimited.

This inquiry made us accomplish the study in 3 universities downtown in Lima : San Marcos Major National University (SMMNU), Federico Villarreal National University (FVNU) and San Juan Bautista Private University (SJBPU), having the goal to propose strategies of information security management and their implications in the quality and accuracy in the services critical of the universities.

It would be mentionated that the sample of the population was made up by 30 experts of the Information and Communication Technology Area (ICT) that work in the three universities mentionated before. A survey form was applied to them to measure their opinions in relation to the security management and services critical.

The results of the research revealed the strategies that should be used in the information security management such as: first, the importance of development security policy : SMMNU 37%, FVNU 19% and SJBPU 24%; second, the programs of personnel training where the experts reported the interest to participate: SMMNU 60%, FVNU 70% and SJBPU 70% and third, the protection to information resource because the 38% of the experts expressed than their information technology centers don´t provide equipment of protection against closing of electric energy, a usual risk in 1980 – 1990 decade.

Also the results demonstrate that to implement these strategies, the impact on the network and web applications will be effective. According to the surveyed experts benefits will be obtained such as : better protection of the information (50%) and better quality on the service for students and teachers (27%). Besides, the risks of information will be minimized because in the case of the SMMNU, the computer virus infection is 56%, the highest from other universities.

According to the security incidents such as: unauthorized modification, unauthorized divulgation and theft information, the results have confirmed what is happening world over, where 70% of these incidents are caused by personnel result of errors, carelessness in theirs knowledge on security or by delinquency acts properly.

On the other hand, we should recommend the University authorities to develop information security policy or to accomplish this policy if they have it because they are the base of a security plan. So, It is convenient an educational program of security conscience related with personnel training. It is also necessary to restructure networks applying prevention technology and intruder detection and separating the academic area from the administrative area because both provide services critical.

Finally, It is recommended a pilot proposal of information security plan to Universities, that will serve for the universities to be taken as a reference to implant their own security plans.

INTRODUCCION

Hoy en día la seguridad va más allá de mecanismos de protección de alta tecnología, ya que sin políticas de seguridad correctamente implantadas en nuestra organización, no sirven de nada los controles de accesos físicos y lógicos a la misma. Se habla ahora de la gestión de seguridad como algo crítico para cualquier organización, igual de importante dentro de la misma como los sistemas de calidad o las líneas de producto que desarrolla.

Precisamente por ello, la presente investigación se orienta a demostrar que una gestión de seguridad de la información basada en políticas de seguridad resultará exitosa si se toma en cuenta todas las necesidades concretas de cada Universidad y que contribuya con eficacia y calidad en los servicios críticos de las Universidades, como son los servicios de Matrícula, Admisión y Registros, Grados y Títulos, Contabilidad y Tesorería e Informática. Estos servicios recopilan información valiosa y confidencial tales como: registro de postulantes, registros de alumnos regulares, certificados de estudios, documentación de Grados y Títulos, bases de datos financieros y presupuestal, registro de direcciones de correo electrónico de alumnos y docentes, etc.

En la presente investigación, hablamos de seguridad de la información y no de seguridad informática, a fin de globalizar el concepto de la información porque ésta puede estar representada de diversas formas: impresa o escrita, almacenada en forma electrónica o magnéticamente. Si bien el objeto de estudio está referido principalmente a temas relacionados con la informática, la forma que posea la información debe usarse y protegerse adecuadamente en las actividades de una institución.

El presente estudio ha sido desarrollado en cinco capítulos; en el primero se presentan los aspectos metodológicos de la investigación, desarrollándose dentro de ella el planteamiento del problema, los objetivos de la investigación, las hipótesis general y específicas, y sus pertinentes variables independientes y dependientes.

En la segunda parte se desarrolla el marco teórico que sustenta la investigación.

En esta se estudia el origen de la información y los atributos principales de la seguridad como son la confidencialidad, la integridad y la disponibilidad. Se estudia la teoría de los sistemas de información y los controles de seguridad. También se resalta las normativas de seguridad tanto nacional como internacional.

En el tercer capítulo se realiza el análisis e interpretación de los resultados obtenidos, para ello fue necesario el uso de programas informáticos y se pudo comprobar las hipótesis planteadas.

En el cuarto capítulo se presenta una propuesta piloto de un plan de seguridad de la información para las universidades, y que servirá de guía para que las universidades puedan tomarla como referencia para la implantación de sus planes de seguridad.

En el último capítulo se precisan las conclusiones arribadas con la presente investigación y las recomendaciones que de ellas se generan, como una forma de contribuir con la gestión de seguridad de la información en las instituciones educativas.

De esta forma, teniendo en cuenta los lineamientos establecidos por la Unidad de Post Grado de la Facultad de Ciencias Administrativas, con esta investigación espero contribuir con los postulados de la Universidad y el desarrollo de las organizaciones de nuestro medio.

CAPITULO I
DISEÑO METODOLOGICO

1.1 PLANTEAMIENTO DEL PROBLEMA

La gestión de la seguridad de una organización puede ser muy compleja, no tanto desde el punto de vista puramente técnico sino más bien desde un punto de vista organizativo. Pensar que en una gran universidad con un número elevado de departamentos, alguien que pertenece a uno de ellos abandona la organización, eliminar su acceso a un cierto sistema no implica ningún problema técnico ya que el administrador sólo ha de borrar o bloquear al usuario de forma inmediata, pero sí va existir graves problemas organizativos.

Un ejemplo para empezar sería de ¿cómo se entera un administrador de sistemas que un cierto usuario, que no trabaja directamente junto a él, abandona la empresa?, ¿quién decide si al usuario se le elimina directamente o se le permite el acceso a su correo durante un mes?, ¿puede el personal del área de seguridad decidir bloquear el acceso a alguien de cierto “rango” en la organización, como un director de departamento, nada más que este abandone la misma?, ¿y si resulta que es amigo del rector, y luego este se enfada? Como vemos, desde un punto de vista técnico no existe ningún escollo insalvable, pero sí que existen desde un punto de vista de la gestión de la seguridad.

Hoy en día, una entidad que trabaje con cualquier tipo de entorno informático, desde pequeñas empresas con negocios no relacionados directamente con las nuevas tecnologías hasta grandes de ámbito internacional, está o debería estar preocupada por su seguridad. Y no es para menos pues el número de amenazas a los entornos informáticos y de comunicaciones crece casi exponencialmente año tras año alcanzando cotas inimaginables hace apenas una década.

Por otra parte la mayoría de redes informáticas en las universidades no fueron diseñadas originalmente pensando en la seguridad. A diferencia de las redes corporativas y otras redes comerciales, que son más cerradas y segmentadas con énfasis en la protección de los recursos valiosos de la información, las redes de la universidad están diseñadas para funcionar como proveedores del servicio de Internet, facilitar el acceso a los usuarios y facilitar el flujo de la información.

Históricamente, el cuerpo docente, los investigadores y estudiantes de las universidades han esperado, y en algunos casos solicitado, acceso gratuito y abierto a los sistemas informáticos universitarios. Sin embargo a la luz de las recientes amenazas y riesgos de la información tales como sabotaje, fraude, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicios, y de las expectativas de más amenazas a la seguridad en el futuro, no puede continuar este acceso abierto e ilimitado.

En muchos aspectos, las universidades recopilan información personal que puede ser mucho más completa, y más confidencial, que aquella del mundo corporativo; por ejemplo, tienen vastas bases de datos financieros , bases de datos de historias clínicas sobre los estudiantes y cuerpo docente , documentación de grados y títulos, registros de notas de los cursos que se dictan, certificados de estudios , etc.

La preocupación de las organizaciones por la seguridad de la información no debe estar centrada sólo en los aspectos más técnicos de la seguridad, sino es necesario proponer a las universidades estrategias de gestión de seguridad de la información que abarque el desarrollo, revisión y cumplimiento de las políticas de seguridad y abordar temas claves de seguridad como la identificación de riesgos críticos, sensibilización, capacitación y privacidad.

Finalmente, para gestionar eficientemente la seguridad de la información se requiere que todos los miembros de la Universidad como autoridades, trabajadores, alumnos y docentes tomen conciencia de la importancia de la seguridad de la información y su papel que juega en generar aportes de calidad y eficacia en los servicios críticos de las Universidades.

1.2 FORMULACION DEL PROBLEMA

1.2.1 Problema principal

¿Qué efectos produce la gestión de seguridad de la información en los servicios críticos de las universidades como son los servicios de Matrícula, Admisión y Registros, Grados y Títulos, Tesorería e Informática?.

1.2.2 Problemas específicos

1. ¿Tienen las universidades estrategias preventivas y planes de contingencia para minimizar los riesgos en el manejo de la información ante incidentes?

2. ¿Cuáles son los beneficios de la gestión de seguridad de la información en los sistemas de información como son la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios en las Universidades?

3. ¿Cómo generar conciencia de seguridad en los trabajadores, estudiantes y docentes sobre la información que manejan en las Universidades?

4. Cómo optimizar el soporte, gestión y seguridad de las redes informáticas de las universidades?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo General

Proponer estrategias de Gestión de Seguridad de la Información y sus implicancias en la calidad y eficacia en los servicios críticos de las Universidades como son los servicios de Matrícula, Admisión y Registros, Grados y Títulos, Tesorería e Informática.

1.3.2 Objetivos Específicos

1. Minimizar los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios con la implementación de políticas de seguridad de la información.

2. Contribuir a la calidad en el servicio y en la protección más segura de los sistemas de información como son la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios de las Universidades

3. Generar conciencia de seguridad en los trabajadores, docentes y alumnos de la Universidad con programas de capacitación para un buen uso de la información.

4. Establecer un nuevo diseño a la red informática universitaria con un tráfico de la información más seguro y un servicio eficaz a los trabajadores, alumnos, docentes y terceros.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

a) Justificación Teórica

La investigación propuesta mediante la aplicación de conceptos y teorías de información dentro del ámbito de seguridad de la información como son los sistemas de información, análisis y gestión de riesgos y cultura de seguridad, busca encontrar explicaciones para contribuir con calidad y eficacia en los servicios críticos de las Universidades.

Para ello se hace necesario desarrollar un marco teórico y conceptual revisando el material bibliográfico existente, contrastando las diversas corriente y posiciones, y a partir de ella comprobar su validez en las Universidades donde tuvimos participación.

b) Justificación Práctica

En la actualidad el tema de la gestión de seguridad de la información y su papel en los servicios críticos de las Universidades es un tema muy importante. Los

recursos de información (sistemas de información, redes, etc.) que sirven como apoyo tanto los profesores, empleados, alumnos y terceros deben emplearlos para su trabajo y estudio, y que no debe estar permitida la utilización de estos recursos con fines comerciales o recreativos. Por ello, los alcances de la investigación tiene repercusión práctica porque aporta información valiosa que servirá como fuente de reflexión y acción para que las autoridades y directivos universitarios analicen los resultados sobre calidad y eficacia en los servicios críticos de las Universidades y a la vez se propone un plan de seguridad de información para las universidades que sirva como modelo para que éstas la puedan aplicar.

c) Metodológica

El tema de la seguridad de la información es reciente y en las Universidades se torna más preocupante por las amenazas a los recursos de su información, por tanto la metodología ha sido la consulta a expertos del área de Tecnología de Información y Comunicaciones de las Universidades de Lima Metropolitana como son la Universidad Nacional Mayor de San Marcos, la Universidad Nacional Federico Villarreal y la Universidad Privada San Juan Bautista.

Para lograr el cumplimiento de los objetivos de la investigación, se acude al empleo de técnicas de investigación. En el trabajo de campo, procesamiento y análisis de los resultados obtenidos fue necesario el uso de las herramientas de aplicación como Microsoft Office, de la misma forma para la preparación y presentación del informe definitivo.

1.5 DELIMITACIÓN DE LA INVESTIGACIÓN

La presente investigación se circunscribe a la consulta de expertos en Tecnología de Información y Comunicaciones que laboran en las Universidades de Lima Metropolitana, la información recolectada corresponde a los meses comprendidos entre Marzo y Mayo de 2006.

1.6 HIPOTESIS DE LA INVESTIGACION

1.6.1 Hipótesis General

La aplicación de estrategias de Gestión de Seguridad de la Información contribuye con calidad y eficacia en los servicios críticos de las Universidades como son los servicios de Matrícula, Admisión y Registros, Grados y Títulos, Tesorería e Informática.

1.6.2 Hipótesis Auxiliares

1. Las Universidades que implementen políticas de seguridad de la información, minimizan los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios.

2. La gestión de seguridad de la información contribuye a la calidad en el servicio y en la protección más segura de los sistemas de información como son la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios en las Universidades

3. Los programas y talleres de capacitación de seguridad de la información crea conciencia de seguridad en los trabajadores, docentes, alumnos y terceros para un buen uso de la información.

4. El rediseño la red informática universitaria permite un tráfico de la información más seguro y un servicio eficaz a los trabajadores, alumnos, docentes y terceros.

1.7 VARIABLES DE LA INVESTIGACION

Variable Independiente

Gestión de seguridad de la información

Variable Dependiente

Servicios Críticos de las Universidades

1.8 OPERACIONALIZACION DE VARIABLES

Las variables obtenidas de nuestras hipótesis las podemos medir con uno o varios indicadores, que se muestran a continuación:

Hipótesis Auxiliar Nº 1

HIPOTESIS	VARIABLES	INDICADORES
Las Universidades que implementen políticas de seguridad de la información minimizan los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios.	VARIABLE INDEPENDIENTE Políticas de seguridad de la información	1. Frecuencia de cumplir con las políticas de seguridad 2. Beneficios de usar políticas de seguridad
	VARIABLE DEPENDIENTE Riesgos en el manejo de la información	1. Frecuencia de riesgos a los recursos de información 2. Incidencias de seguridad por los usuarios

Hipótesis Auxiliar Nº 2

HIPOTESIS	VARIABLES	INDICADORES
La gestión de seguridad de la información contribuye a la calidad en el servicio y en la protección más segura de los sistemas de información como son la matrícula de alumnos, admisión y registros, tesorería y trámites documentarios en las Universidades	VARIABLE INDEPENDIENTE Gestión de seguridad de la información	1. Frecuencia de la importancia de las medidas de seguridad de la información
	VARIABLE DEPENDIENTE Servicio eficaz y tráfico de información más seguro de los sistemas de información	2. Nivel de gestión de seguridad de la información en los servicios académicos y administrativos

Hipótesis Auxiliar Nº 3

HIPOTESIS	VARIABLES	INDICADORES
Los programas y talleres de capacitación de seguridad de la información crean conciencia de seguridad en los trabajadores, docentes, alumnos y terceros para un buen uso de la información.	VARIABLE INDEPENDIENTE Programas y talleres de capacitación	1. Frecuencia de asistencia a programas de capacitación 2. Grado de interés del personal por capacitación
	VARIABLE DEPENDIENTE Conciencia de seguridad a trabajadores, docentes, alumnos y terceros	1. Grado de interés del personal por capacitación

Hipótesis Auxiliar Nº 4

HIPOTESIS	VARIABLES	INDICADORES
El rediseño la red informática universitaria permite un tráfico más seguro de la información y un servicio eficaz a los trabajadores, alumnos docentes y terceros.	VARIABLE INDEPENDIENTE Rediseño de la red informática universitaria	1. Nivel de conocimiento sobre el diseño de redes informáticas universitarias
	VARIABLE DEPENDIENTE Servicio eficaz y tráfico de información más seguro de los sistemas de información	1. Nivel de Gestión de seguridad en los servicios académicos y administrativos

1.9 ASPECTOS METODOLOGICOS

1.91 Tipo de Nivel de Investigación

La presente investigación es de carácter descriptivo, debido a que su propósito es la formulación de un problema, y proponer estrategias en la gestión de la seguridad de los servicios críticos de las Universidades como son los servicios de Matrícula, Admisión y Registros, Grados y Títulos, Tesorería e Informática, y así posibilitar una investigación más precisa o el desarrollo de una hipótesis.

Además, cabe resaltar que a través de fuentes de información de otros autores como monografías e investigaciones bibliográficas, nos ha ayudado a reunir y sintetizar experiencias, y a la vez que se aclaren conceptos sobre el nivel de conocimiento científico desarrollado previamente por estos trabajos y poder catalogar este tipo de estudio.

1.9.2 Población y Muestra

- De las 24 universidades de Lima, 5 son públicas y 19 privadas. El universo de la investigación se encuentra conformado por expertos en el área de Tecnología de Información y Comunicaciones de las Universidades de Lima Metropolitana que están involucrados con temas de la seguridad de la información.

- La muestra se determinó teniendo en cuenta el universo de expertos del área de TIC como son los Directores, Jefes, Administradores de Redes, Administradores de Base de Datos, Administradores Web, Administradores de Redes y Comunicaciones y Jefes de Laboratorio de computadoras. La muestra se refleja en el siguiente cuadro:

Universidades	Personal de TIC
Universidad Nacional Mayor de San Marcos	10
Universidad Nacional Federico Villarreal	10
Universidad Privada San Juan Bautista	10
Total	**30**

- Se tomó como casos de estudio a la Universidad Nacional Mayor de San Marcos y a la Universidad Nacional Federico Villarreal porque son universidades representativas de las universidades públicas y a la Universidad Privada San Juan Bautista por la facilidad en la accesibilidad de la información.

1.9.3 Diseño de la Investigación

Se realizaron encuestas para las 3 Universidades mencionadas. En el Anexo Nº 1 se muestra el diseño de la encuesta.

1.9.4 Técnicas e instrumentos de Recolección e Datos

El **cuestionario** se aplicó al personal experto de TIC que se seleccionó en la muestra, la cual estableció las consecuencias lógicas de los objetivos e hipótesis planteados.

1.9.5 Tratamiento y procesamiento de los datos

Se procedió a la codificación y tabulación de la información para el recuento, clasificación y ordenación de la información en tablas.
Una vez que se obtuvo la información tabulada se procedió a procesarla mediante las herramientas de Microsoft Office.

CAPITULO II
MARCO TEORICO

2.1 ANTECEDENTES DE LA INVESTIGACION

La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) consciente de la modernización de las organizaciones públicas en el Gobierno Electrónico que requieren un enfoque más agudo en seguridad de la información, emitió la primera encuesta nacional sobre seguridad de la información con RM-310-2004 (Anexo Nº 2).

La Primera Encuesta de Seguridad de la Información en la Administración Pública, fue aplicada a las entidades públicas como poderes del Estado, organismos autónomos y gobiernos locales[1].

Dentro de los puntos más relevantes de la encuesta se ha observado que:

- El 63% no posee un responsable en temas de seguridad de la información.
- El 86% no cuenta con asesoramiento en temas de seguridad de la información.
- El 59% de instituciones no prepara a sus usuarios para reportar incidentes de seguridad.
- El 82% no recibe capacitación en temas de seguridad.
- El 70% no tiene preparados procedimientos de respuesta a incidentes o anomalías que pudieran suceder.

Con fecha 23 de Julio de 2004 la Presidencia del Consejo de Ministro a través de la Oficina Nacional de Gobierno Electrónico e Informático, dispone de uso obligatorio de la Norma Técnica Peruana: "NTP – ISO 17999:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información" en las entidades del Sistema Nacional de Informática[2], dicha norma se basa en el estándar internacional ISO 17799 que es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector.

---

[1] OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA . *Primera encuesta de Seguridad de la Información en la Administración Pública*. [En línea] http://www.ongei.gob.pe/publicaciones/IEncuestadeSeguridad.pdf. [Consulta: 10 de Octubre de 2006]

[2] OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA. *Norma Técnica Peruana.* [En línea].www.ongei.gob.pe/bancos/banco_normas/archivos/P01-PCM-ISO**17799**-001-V1.pdf . [Consulta: 10 de Octubre de 2006]

Córdova[3], realizó una investigación titulada “Plan de Seguridad Informática para una Entidad Financiera”, donde se hace un diagnóstico de la situación actual en cuanto a su estructura interna y a la seguridad de la información que la entidad financiera actualmente administra y diseñar un Plan de Seguridad de la Información que permita desarrollar operaciones seguras basadas en políticas y estándares claros y conocidos por todo el personal de la entidad. Este trabajo describe en detalle cómo diseñar el plan de seguridad de la información para lo cual se realiza una evaluación de riesgos y vulnerabilidades a los que está expuesta la entidad, luego se desarrollan políticas y estándares de seguridad de la información con el fin de contar con una guía para la protección de la información. Para controlar las conexiones de la red de la entidad financiera con entidades externas y monitorear la actividad realizada a través de dichas conexiones, se ha propuesto una arquitectura de red la cual incluye dispositivos de monitoreo de intrusos. Finalmente el plan de implementación describe la actividad a ser realizada, las etapas incluidas en su desarrollo y el tiempo estimado en su ejecución.

Rodríguez Hernández[4], realizó un informe titulado “Arquitectura de Seguridad de la Red Inalámbrica Universitaria”, donde a partir de la iniciativa de la Universidad Autónoma de México para dotar al campus universitario de una red inalámbrica se hizo evidente la necesidad por parte del Departamento de Seguridad de Cómputo la responsabilidad de aportar al proyecto los mecanismos que garantizaran una operación de la red que feira segura y a la vez eficiente. Las actividades que se llevaron a cabo fueron la creación de políticas de uso aceptable, las políticas de monitoreo, el análisis de riesgo, mapeo de redes inalámbricas, la selección del esquema de autenticación y control de acceso.

El proyecto está planteado para dar cobertura inicialmente a las escuelas, facultades, institutos, centros de investigación, bibliotecas, recintos culturales y áreas de congregación de estudiantes e investigadores universitarios en la ciudad universitaria e irá creciendo conforme la demanda y los servicios los soliciten. El hecho de haber considerado a la Red Inalámbrica Universitaria (RIU) desde su diseño tendrán beneficios que se reflejarán en el control de la infraestructura, la contención de daños en el caso de

[3] CORDOVA RODRIGUEZ, Norma. *Plan de seguridad informática para una entidad financiera*. [En línea] http://sisbib.unmsm.edu.pe/bibvirtual/Tesis/Basic/cordova_rn/cordova_rn.htm[Consultado: 10 de Diciembre de 2006]

[4] RODRIGUEZ HERNANDEZ, Eduardo. *Arquitectura de Seguridad de la Red Inalámbrica Universitaria*. [En línea]. http://www.astralix.com/papers/riu-titulacion-espina.pdf. [Consultado: 10 de Diciembre de 2006]

un incidente y un tiempo de respuesta menor. La RIU tampoco es un proyecto estático, sino que irá transformándose según las necesidades de la comunidad universitaria, por ello se han considerado metodologías que permiten escalar de una forma organizada las actualizaciones tecnológicas.

Rodríguez López[5], realizó una investigación titulada: "La influencia de la cultura organizacional en la implantación de la estrategia de seguridad de la información en una organización financiera", donde manifiesta que el tema de la seguridad de la información ha tenido un fuerte crecimiento en los últimos años, debido a la gran apertura y a la globalización que se han enfrentado todas las organizaciones y que el objetivo de esta investigación radica en la identificación del impacto de la cultura organizacional en la implantación de una estrategia de seguridad de la información, su efectividad enfocado a una organización del sector financiero y sus aspectos más relevantes. A través de un trabajo de campo se llegaron a las siguientes conclusiones: se comprobó que existe una relación directa entre la efectividad del establecimiento de una estrategia de protección de la información y la cultura organizacional en la organización del sector financiero. La cultura organizacional dificulta la implantación de una estrategia de protección de información relacionada con la seguridad de la información, debido a que la cultura tradicionalista es muy arraigada y ha significado un factor que ha impedido la efectividad de la misma. La cultura actual piensa que está poniendo en tela de juicio y rompiendo un paradigma que hasta ahora había sido el pilar dentro de esta organización, lo cual era la confianza en los empleados que laboran en la misma. Es necesaria una evaluación global de la situación, estableciendo planes de acción conjuntos buscando metas muy específicas y a plazos cortos, teniendo el apoyo de las personas relacionadas directamente con la implementación. Finalmente es necesario el apoyo de los directores de las diferentes áreas y mayor presupuesto para hacer campañas y talleres donde puedan ver y sentir algunos de los impactos de no respetar las normas y como se pueden presentar las violaciones a estas reglas, esto podría enriquecer el dominio e interés de cada persona a fin de enfocar a esta cultura.

[5] RODRIGUEZ LOPEZ, Margarita. *La influencia de la cultura organizacional en la implantación de la estrategia de seguridad de la información en una organización financiera*. [En línea] http://www.bib.uia.mx/tesis/pdf/014510/014510.pdf.[Consultado: 15 de Enero de 2007]

Domingo[6], en el estudio titulado “Seguridad en las transacciones on line de comercio electrónico” , manifiesta que la seguridad en la web es difícilmente absoluta, pero se puede minimizar el riesgo utilizando medidas de seguridad adecuadas y planes para una recuperación ante incidentes de seguridad. La seguridad debe ser parte integral de una organización. El desarrollo de políticas de seguridad y su aplicación posibilita evitar muchos problemas potenciales. Es necesario producir un cambio de cultura en aquellas organizaciones en las que es preciso que las cosas ocurran para que se planifiquen las acciones a seguir. En este trabajo se analizó la barrera de muchas empresas de comercio electrónico que quieren expandir sus límites y pese a sus esfuerzos en el marketing del producto, fracasan por miedos, inseguridades y errores tecnológicos. Se entrevistó a profesionales del área de sistemas que son usuarios del comercio electrónico. Si bien el 80% de los consultados considera que el comercio electrónico ha cambiado la forma de comprar por el acceso a las ofertas, el 95% de los profesionales alegan estar preocupados por la seguridad y en transmitir a los clientes la sensación de seguridad pero admiten no conocer en profundidad los procesos que la aumentan tangiblemente y no poder ponerlas en práctica a sus proyectos en TI.

2.2 BASES TEORICAS

2.2.1 La Administración

En una época de complejidades, cambios e incertidumbres como se vive actualmente, la administración se ha convertido en una de las áreas más importantes de la actividad humana. La tarea básica de la administración es hacer las cosas por medio de las personas de manera eficaz y eficiente. En las organizaciones, la eficiencia y la eficacia con que las personas trabajan en conjunto para conseguir objetivos comunes depende directamente de la capacidad de quienes ejercen la función administrativa. El avance tecnológico y el desarrollo del conocimiento humano, por sí solos, no producen efectos si la calidad de la administración sobre los grupos organizados de personas no permite la aplicación efectiva de los recursos humanos y materiales.

---

[6] DOMINGO, Gonzalo Ernesto. *Seguridad en las transacciones on line de comercio electrónico*. [En línea] http://www.eiidi.com/Download/**Seguridad**%20de%20**transacciones**%20en%20**line**a.pdf [Consultado: 15 de Diciembre de 2006]

A continuación mencionamos a algunos autores de renombre mundial sobre el papel que cumple la Administración:

Para Koontz[7], la administración es el proceso de diseñar y mantener un entorno en el que trabajando en grupos, los individuos cumplan eficientemente objetivos específicos. Todos administran organizaciones, a las que definiremos como un grupo de personas que trabajan en común para generar un superávit. En las organizaciones comerciales, este superávit son las utilidades. En las organizaciones no lucrativas, el superávit puede estar representado por la satisfacción de las necesidades. Las universidades también generan un superávit por medio de la creación y difusión de conocimientos, así como la prestación de servicios a la comunidad o sociedad.

Según Chiavenato[8], la Administración es la manera de integrar las organizaciones o parte de ellas. Es el proceso de planear, organizar, dirigir y controlar el uso de los recursos organizacionales para alcanzar determinados objetivos de manera eficiente y eficaz.

Para Stoner y Freeman[9], la Administración es el proceso de planificación, dirección y control del trabajo de los miembros de la organización y de usar recursos disponibles de la organización para alcanzar las metas establecidas. La Administración consiste en darle forma, de manera consciente y constante, a las organizaciones.

Para Peter Drucker, la Administración es una disciplina social que se dedica al comportamiento de las personas e instituciones humanas, cuyos supuestos básicos son en realidad más importantes que los paradigmas para una ciencia natural.

Peter Drucker, citado por Chiavenato[10], afirma que no existen países desarrollados ni países subdesarrollados, sino países que saben administrar la tecnología, los recursos disponibles y potenciales, y países que todavía no saben hacerlo. En otros términos, existen países administrados y países subadministrados. Lo mismo ocurre en las

[7] KOONTZ, Harold y Heinz Weihrich. *Administración. Una perspectiva global*. McGRAW-HILL. México. 2004.
[8] CHIAVENATO, Idalberto. *Introducción a la teoría general de la administración.* McGRAW-HILL. México. 2006.
[9] STONER, James y Edward Freeman. *Administración.* Prentice-Hall-Hispanoamericana S.A. México. 1996.
[10] CHIAVENATO, Idalberto. *Introducción a la teoría general de la administración.* McGRAW-HILL. México. 2006.

organizaciones. Existen organizaciones excelentes y organizaciones precarias de administración. Todo se reduce a un aspecto de talento administrativo.

Proceso administrativo

Desde finales del siglo XIX se acostumbra a definir la administración en términos de cuatro funciones específicas: la planeación, la organización, la dirección y el control.

Según Stoner[11], un proceso es una forma sistemática de hacer las cosas. Así, la administración es un proceso por cuanto todas las personas que administran, sean cuales fueren sus aptitudes o habilidades personales, desempeñan ciertas actividades interrelacionadas con el propósito de alcanzar las metas establecidas para la organización.

A continuación describimos las funciones o actividades básicas del proceso administrativo:

- **Planeación:** La planeación incluye la selección de misiones y objetivos y las acciones para lograrlos; requiere tomar decisiones, es decir, seleccionar cursos futuros de acción entre varias opciones. No existe un plan real hasta que se haya tomado una decisión: un compromiso de recursos humanos, materiales o reputación. Antes de tomar una decisión todo lo que existe es un estudio de planeación, un análisis o una propuesta.
- **Organización:** La organización es aquella parte de la administración que implica establecer una estructura intencional de los papeles que deben desempeñar las personas en una organización. La estructura es intencionada en el sentido de que debe garantizar la asignación de todas las tareas necesarias para el cumplimiento de las metas, asignación que debe hacerse a las personas mejor capacitadas para realizar esas tareas.

  El propósito de una estructura organizacional es contribuir a la creación de un entorno favorable para el desempeño humano. Se trata, entonces de un instrumento administrativo, no de un fin en si mismo.

[11] STONER, James y Edward Freeman. *Administración.* Prentice-Hall-Hispanoamericana S.A. México. 1996.

- **Dirección:** La dirección es el hecho de influir en los individuos para que contribuyan a favor del cumplimiento de las metas organizacionales y grupales; por lo tanto, tiene que ver con el aspecto interpersonal de la administración. Todos los administradores coincidirían en que sus problemas más importantes son los que resultan de los individuos y en que los administradores eficaces deben ser al mismo tiempo líderes eficaces.
- **Control:** El control consiste en medir y corregir el desempeño individual y organizacional para garantizar que los hechos se apeguen a los planes. Implica la medición del desempeño con bases en metas y planes, la detección de desviaciones respecto de las normas y contribución a la corrección de éstas. Así, el control facilita el cumplimiento de los planes. Aunque la planeación debe preceder al control, los planes no se cumplen solos. Los planes orientan a los administradores en el uso de recursos para la consecución de metas específicas, tras de lo cual las actividades son objeto de revisión para determinar si responden a lo planeado.

Henry Fayol, conocido como "el padre de la teoría administrativa moderna", citado por Rodríguez Valencia[12], estableció que toda empresa debería realizar las funciones comerciales, técnicas, financieras, seguridad, contable y administrativas. Identificó a la seguridad como una de las actividades fundamentales de la empresa y que tiene como misión proteger los bienes y las personas contra accidentes, y todos los obstáculos de orden social que pueden comprometer la marcha y hasta la vida de la empresa.

Considerando el papel que cumple la administración, una gestión de seguridad debe contemplar procedimientos adecuados y la planeación e implantación de controles de seguridad basadas en una evaluación de riesgos y una medición de la eficacia de los mismos.

2.2.2 La Gestión de seguridad de la información

La gestión de la seguridad de la información consiste en garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible,

[12] RODRIGUEZ VALENCIA, Joaquín. *Administración I.* Thomson Learning Ibero. México. 2006.

eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

2.2.2.1 La seguridad

> *"Seguridad viene a ser la protección de los activos frente acciones o situaciones no deseadas, mediante la implantación de los controles, lo que suele suponer una inversión y un esfuerzo. Y todo ello en las entidades para proteger los intereses de los accionistas, de los empleados, de los clientes, de los proveedores y de los ciudadanos afectados según el sector como alumnos o pacientes."*[13]

La seguridad es hoy día una profesión compleja de funciones especializadas. Los sistemas de seguridad son cada vez más automáticos, particularmente aquellos de detección y comunicación de siniestros y aquellos relacionados con la valoración, la decisión y la reacción. Importantes compañías tienen su organización interna de seguridad, además que son disponibles para cualquier persona una serie de servicios de seguridad ofrecidos por compañías privadas. Todo esto ha contribuido a atraer más personas interesadas en la materia, y a provocar una atención del mundo de los negocios y de los gobiernos.

Por otra parte, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se puedan incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad. En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concienciación respecto a la importancia de la información y el conocimiento en este nuevo milenio.

[13] PESO NAVARRO, Emilio del. *El Documento de Seguridad* .Díaz de Santos. 2004.

2.2.2.2 La información

La Enciclopedia Wikipedia[14], define a la información como un fenómeno que proporciona significado o sentido a las cosas, e indica mediante códigos y conjuntos de datos, los modelos del pensamiento humano. La información por tanto, procesa y genera el conocimiento humano. Los datos, en cambio, son flujos de hechos que representan sucesos ocurridos en las organizaciones o en el entorno físico, antes de ser organizados y acomodados de tal forma que las personas puedan entenderlos y usarlos. Los datos se perciben mediante los sentidos, éstos los integran y generan la información necesaria para producir el conocimiento que es el que finalmente permite tomar decisiones para realizar las acciones cotidianas que aseguran la existencia social

En otros términos, podemos decir que los datos son cifras y hechos crudos, sin analizar. La información, por otra parte, es el resultado de haber organizado o analizado los datos de alguna manera y con un propósito.

"La información es el recurso clave para quien trabaja con el conocimiento en general, y especialmente para el ejecutivo. Cada vez más, la información crea el eslabón con sus colegas y con su organización y con su "red". En otras palabras, la información es lo que permite que aquéllos que trabajan con el conocimiento lleven a cabo su labor. Por otra parte, solamente los que trabajan con el conocimiento, como individuos, y especialmente los ejecutivos como individuos, pueden decidir cómo organizar su información para convertirla en su clave para una acción eficaz, pues mientras no está organizada la información sigue siendo datos."[15]

Historia de la información

- En la Edad Media el almacenamiento, acceso y uso limitado de la información se realizaba en las bibliotecas de los monasterios entre los siglos III y XV.
- En la Edad Moderna, con el nacimiento de la imprenta (Gutemberg), los libros podían fabricarse en serie. Surgen los primeros periódicos.
- En el siglo XX, Claude E. Shannon, un ingeniero nacido en Michigan en 1916, publicó en 1948 algunos trabajos relacionados con el tratamiento de la

[14] ENCICLOPEDIA WIKIPEDIA. [En línea] http://es.wikipedia.org/wiki/Universidad [Consulta: 10 de Enero de 2007]
[15] DRUKER, F. Peter. *Los desafíos de la Gerencia para el siglo XX*!. Norma. Bogotá. 1999.

información (teoría de la información). Durante este siglo irrumpe la radio, la televisión.

- James Watson y Francis Crick descubrieron los principios de los códigos de ADN, que forman un sistema de información a partir de la doble espiral de ADN y la forma en que trabajan los genes.
- En los años 40, Jeremy Campbell, definió el término información desde una perspectiva científica, en el contexto de la era de la comunicación electrónica.
- Norbert Wiener, padre de la cibernética, se encargó de "mantener el orden" en cualquier sistema natural o artificial. Estos avances dieron lugar a una nueva etapa en el desarrollo de la tecnología, en la cual muchos científicos se inspiraron en estos estudios para hacer sus propios aportes a la teoría de la información.
- Actualmente, ya en el siglo XXI, en un corto período de tiempo, el mundo desarrollado se ha propuesto lograr la globalización del acceso a los enormes volúmenes de información existentes en medios cada vez más complejos, con capacidades ascendentes de almacenamiento y en soportes cada vez más reducidos. La proliferación de redes de transmisión de datos e información, de bases de datos con acceso en línea, ubicadas en cualquier lugar, localizables mediante Internet, permiten el hallazgo de otras redes y centros de información de diferentes tipos en cualquier momento desde cualquier lugar.

2.2.2.3 La seguridad de la información

La información es un activo que tiene un valor fundamental para la organización y debe ser protegida de un modo adecuado. Así, la seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar las oportunidades de negocio.

Podríamos definir la seguridad de la información como un conjunto de sistemas y procedimientos que se caracteriza como la preservación de:

a) **su confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información;
b) **su integridad**, asegurando que la información y sus métodos de proceso son exactos y completos;

c) **su disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

A través de un ejemplo práctico sobre los principios de la seguridad de la información el autor Oscar Schmitz[16] menciona lo siguiente: *"Si alguien roba un activo de información (laptop, informe, disquete, etc.), una persona no autorizada podría leer y difundir la información contenida. Desde esta situación podemos aseverar, en principio, que esta en peligro la confidencialidad de la información. Ahora si la persona no autorizada, corrompe, modifica o borra la información contenida, impactaría directamente en problemas de integridad. Finalmente, si la información contenida no fue copiada en otro soporte a modo de resguardo (backup), podrían sucederse problemas de disponibilidad, dado que ninguna persona accedería a esta información. "*

La confidencialidad tiene sus propias características según Molina Mateos[17] citado por Arturo Ribagorda:

> *"1.- Propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados. Según esta norma la confidencialidad es un servicio de seguridad.*
>
> *2.- Prevención de la revelación no autorizada de información.*
>
> *3.- Característica de los datos e informaciones que son revelados sólo a los usuarios, entidades o procesos en el tiempo y forma autorizados."*

Asimismo, Molina Mateos[18] menciona que existe información que por su importancia vital para la organización constituye un activo estratégico, y cuya pérdida puede llegar a ser gravemente perjudicial, e incluso letal, para la misma, mientras que otras, aun manteniendo el valor intrínseco atribuible a toda información en un sentido genérico, incorporan un valor de menor entidad cuya pérdida produce efectos o perjuicios de efectos menos significativos.

---

[16] SCHMITZ, Oscar. *Principios básicos de seguridad de la información* [En línea] http://conosur.cio.com/?q=node/16. [Consultado: 15 de Enero de 2007]

[17] MOLINA MATEOS, José María. *Criptología y Derecho. Colección Seguridad de la Información y Derecho*. El Cid Editor, 2000.

[18] MOLINA MATEOS, José María. *Seguridad de la información. Criptología*. El Cid Editor. Madrid. 2000.

Según Del Peso Navarro[19], a la hora de implantar medidas de seguridad, es preciso tener hecha una clasificación de la información conociendo lo que realmente debemos proteger y lo que no, y no adoptando medidas iguales para todo nuestro patrimonio informacional, cuando, en muchos casos, parte de él no merece que realicemos ningún gasto de seguridad,

Por ello, la información, como activo de cualquier organización, ha de ser clasificada según el grado de sensibilidad e importancia para la misma y, en base a ello, poder definir la que debe ser protegida y con qué niveles.

2.2.2.3.1 Necesidad de la seguridad de la información

La información y los procesos que la apoyan, sistemas y redes son importantes activos de la organización. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez mas, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informáticas, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Gene Spafford, citado por el consultor Vicente Aceituno[20] es muy preciso al señalar que *" El único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón , rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces yo no apostaría mi vida por ello."*

Peso Navarro[21] menciona que en un principio, la información estaba recluida en unas salas, verdaderos templos dentro de las empresas y de las Administraciones Públicas, su protección era relativamente fácil, prácticamente consistía en defender

[19] PESO NAVARRO, Emilio del. *Servicios de la sociedad de la información*. Díaz de Santos. Madrid. 2003.
[20] ACEITUNO, Vicente. *Definición de seguridad de la información y sus limitaciones*. [En línea] http://www.fistconference.org/data/presentaciones/queesseguridad.pdf. [Consulta :08 Mayo de 2006]
[21] PESO NAVARRO, Emilio del. *Servicios de la sociedad de la información*. Ediciones Díaz de Santos. Madrid 2003.

físicamente el recinto del Centro de Proceso de Datos y eran pocos los miembros en acceder a esos datos informatizados. En una segunda fase, la información empezó a salir y a circular por toda la empresa a través de las redes de comunicación. Asimismo, el número de personas que podía acceder a los datos informatizados aumentó considerablemente; aunque con ciertas restricciones. El tercer salto ocurrió con la aparición de los ordenadores personales y la utilización generalizada de las redes públicas o el Internet. La aparición y utilización masiva de Internet ha hecho que el tema de la seguridad en la sociedad de la información sea prioritario a la hora de buscar soluciones.

El autor Kennet Laudon[22] sostiene que antes de la automatización con computadoras, los datos acerca de individuos y organizaciones se mantenían y protegían en forma de expedientes en papel dispersos en distintas unidades de negocios o de organización. Los sistemas de información concentran los datos en archivos de computadoras a los que podrían tener fácil acceso un gran número de personas y grupos externos de la organización.

Muchos de los sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización.

2.2.2.3.2 Requisitos de seguridad

a) Evaluación de los riesgos de seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el posible impacto económico, resultante de los fallos de seguridad. Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, sólo a parte de ella o incluso a sistemas de información individuales, a componentes específicos o a servicios dónde sea factible, realista y útil.

[22]LAUDON, Kennet y Jane LAUDON. *Sistemas de Información Gerencial*. Octava edición, Pearson Educación de México, 2004.

La evaluación del riesgo es una consideración sistemática;

- del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos;
- de la probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados.

El autor Shinder[23] señala que se deben determinar tanto la naturaleza como el nivel de los riesgos de seguridad para la organización, los cuales se describen a continuación:

- Determinar los tipos de brechas de seguridad a los que es vulnerable la organización.
- Para cada uno de los posibles tipos, determinar la posibilidad de que se produzca la brecha en la seguridad.
- Para cada uno de los posibles tipos, determinar la extensión de las pérdidas que se producirían de darse la brecha.

Este proceso se conoce como análisis cuantitativo de riesgos. Otro tipo de análisis de riesgos, el *análisis cualitativo de riesgos,* rechaza el elemento de probabilidad, centrándose en su lugar en las amenazas potenciales y en las características de la red o el sistema que pueden ser vulnerables ante dichas amenazas, para desarrollar posteriormente métodos para prevenir o reducir la probabilidad de las brechas, detectar cuándo se producen y reducir y reparar los daños producidos en caso de que se produzca la brecha.[24]

Los resultados de esta evaluación ayudarán a encauzar y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de la seguridad de la información, y la implantación de los controles seleccionados para protegerse contra dichos riesgos.

[23] SHINDER Debra Littlejhon. *Prevención y Detección de delitos informáticos*. Anaya Multimedia, Madrid. 2003.
[24] SHINDER Debra Littlejhon. Prevención y Detección de delitos informáticos. Anaya Multimedia, Madrid. 2003.

b) Controles de seguridad

El autor Molina Mateos[25] señala que la amplificación de los efectos de la información por el uso de las nuevas tecnologías comporta un incremento paralelo de las oportunidades para su violación, con escasa o nula posibilidad de hacer reversible el daño causado y grandes dificultades probatorias, que demanda un sistema de prevención real y efectivo. Una prevención efectiva ante estas agresiones son las estructuras jurídicas que tutelen a los ciudadanos frente a eventuales agresiones tecnológicas a sus derechos pero también puede provocar que bajo el pretexto de conductas antisociales o incluso ilícitas se multiplique los obstáculos para el ejercicio de las libertades.

Una política de seguridad se define como un documento escrito que representa el enfoque de seguridad de una organización o de un área de seguridad específica y que establece una serie de normas que deben seguirse al aplicar la filosofía de seguridad de la organización. Las políticas de seguridad son la base de un plan de seguridad de una organización

Para los autores Peso Navarro y Ramos González[26], la seguridad de la información sigue dependiendo del elemento humano, de la cultura de seguridad, de la formación e información, y de la motivación de las personas, a veces en mucha mayor medida que de cuantiosas inversiones en sofisticados dispositivos o software de control de accesos.

La mentalización necesaria puede iniciarse o propiciarse a partir de las políticas. Si no hay políticas, la seguridad nunca podrá ser corporativa, además con las políticas se puede hacer patente el soporte que existe por parte de la Alta Dirección respecto a un tema, como puede ser en este caso la importancia de la información y su protección en la entidad.

[25] MOLINA MATEOS, José María. *Criptología y Derecho. Colección Seguridad de la Información y Derecho*. El Cid Editor. Madrid. 2000.
[26] PESO NAVARRO, Emilio del y Miguel Angel RAMOS GONZALEZ. *La seguridad de los datos de carácter personal*. Díaz de Santos. Madrid. 2002.

Así mismo, Gaspar[27] menciona que "*la seguridad debe formar parte de los objetivos estratégicos de la organización, y la Implantación de la Continuidad del Negocio debe estar enmarcada dentro de esos objetivos. Un plan de continuidad de negocio no puede plantearse nunca como un proyecto que tenga una rentabilidad medible, y menos a corto plazo"*

Calle Guglieri[28] menciona que la política de la seguridad de una compañía es proporcionar a los órganos gestores de la misma, a través de un documento escrito, la orientación y soporte adecuados para poder garantizar la seguridad de la información tratada y transmitida por la compañía. Así mismo un aspecto muy importante en la preparación y realización de un plan de seguridad es la participación de compañías y consultores de seguridad externos, naturalmente con los debidos compromisos y controles de confidencialidad registrados por escrito.

Corroboran la afirmación anterior dos hechos fundamentales:

- La experiencia de compañías y consultores de seguridad pueden ahorrar no sólo mucho dinero, lo cual ya es importante sino también mucho tiempo, lo cual puede ser mucho más importante hoy día.
- La visión de los problemas de la compañía, y las consiguientes recomendaciones para paliarlos, son más objetivas y desinteresadas. En particular, suelen servir de catalizadores para unificar criterios y recursos en las "islas" de conocimientos, sistemas y productos que suelen formarse en las grandes compañías.

"*Uno de los componentes más preocupantes para el cliente es la forma en que el suministrador de servicio va a manejar la seguridad tanto de los servicios como de la propia información, así como la posible degradación en sí misma de la propia seguridad. En el contrato de outsourcing deben constar claramente las exigencias de seguridad. Indudablemente el medio idóneo para ello es tener fijadas de antemano en la organización unas políticas de seguridad desarrolladas en sus correspondientes estándares, guías y procedimientos".*[29]

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y

[27] GASPAR, Juan. *Planes de Contingencia.* Díaz de Santos. Madrid. 2004.
[28] CALLE GUGLIERI, José A. *Reingeniería y Seguridad en el Ciberespacio*. Díaz de Santos. Madrid. 1996.
[29] PESO NAVARRO, Emilio del. *Manual de Outsourcing Informático*. Díaz de Santos. Madrid. 2003.

funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

Estándares de la Seguridad de la Información

Toda organización que haga uso de las tecnologías de información se recomienda implementar buenas prácticas de seguridad, pues en muchas ocasiones el no seguir un proceso de implementación adecuado puede generar vacíos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información.

El origen del primer estándar en seguridad de la información fue desarrollado en los años 1990, en Inglaterra, como respuesta a las necesidades de la industria, el gobierno y las empresas para fomentar un entendimiento común sobre el tema y establecer lineamientos generales. En 1995, el estándar BS 7799 es oficialmente presentado. En 1998 se establecen las características de un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita un proceso de certificación, conocida como BS 7799 parte 2.

Recién en diciembre del 2000 la organización de estándares internacionales (ISO) incorpora la primera parte de la norma BS 7799, rebautizada como ISO 17799, la cual se presenta bajo la forma de notas de orientación y recomendaciones en el área de Seguridad de la información.

En el año 2005 hubo cambios interesantes a nivel de ISO 17799 y de COBIT (con su nueva versión 4.0). En cuanto a la norma ISO, las novedades son más que interesantes. Hasta ahora muchas compañías se alineaban a la 17799:2000 y luego tenían que certificar la norma BS 7799:2002 dado que ISO no había reglamentado las características de un Sistema de Gestión de Seguridad de la Información.

La buena noticia es que a partir de ahora se podrá certificar con la nueva norma ISO/IEC27001. Entonces, hoy el marco teórico es la ISO/IEC 17799:2005 y el marco práctico pasó a ser la ISO/IEC 27001:2005[30] (Anexo Nº 3). Esta última define el Sistema de Gestión de la Seguridad de la Información (SGSI).

[30] EL PORTAL DE ISO 27000 EN ESPAÑOL. [En línea] http://www.iso27000.es/iso27000.html. [Consulta: 15 de Enero de 2007].

Por otra parte, a nivel mundial, Japón es el país que cuenta con el mayor número de certificaciones de seguridad de la información, en total son 1910. A nivel nacional Telefónica Empresas Perú[31], obtuvo la certificación ISO-27001:2005 para su proceso de Gestión de Redes y Servicios, convirtiéndose en la primera empresa peruana en lograr esta certificación y la primera de telecomunicaciones en Latinoamérica. Los requisitos establecidos por la norma internacional ISO-27001:2005 acreditan que la información utilizada en el proceso de Gestión de Redes y Servicios de Telefónica Empresas es administrada con confidencialidad, integridad y disponibilidad, cumpliendo los más altos estándares ofrecidos sólo por empresas líderes del primer mundo. La implantación de esta norma promueve y garantiza una cultura de mejores prácticas en la gestión de la seguridad de la información de los clientes y de nuestra organización, con la premisa de que la información es el principal activo de las empresas y por lo tanto el más valioso.

La certificación se obtuvo luego de un planificado proceso de análisis, diagnóstico e implantación del Sistema de Gestión de Seguridad de la Información, en estricto cumplimiento de los lineamientos ISO y cada uno de los 133 requisitos de la norma 27001: 2005.

2.2.2.3.3 Seguridad de los sistemas de información

"Un sistema de información adecuado ha de incluir información que obliga a los ejecutivos a formular las preguntas correctas, y no limitarse a alimentarlos con la información que ellos esperan. Esto presupone que los ejecutivos saben qué información necesitan. Precisa, además, que obtengan dicha información con regularidad. Por último, exige que integren la información sistemáticamente en su toma de decisiones".[32]

Los sistemas de computación juegan un papel crucial en las empresas, el gobierno y la vida diaria que las organizaciones deben dar pasos especiales para proteger sus sistemas de información y asegurar de que sean exactos confiables y seguros. Cuando se almacenan grandes cantidades de datos en forma electrónica, éstos son vulnerables a muchos tipos de amenazas a las que no están expuestos los datos asentados en papel.

[31] TELEFÓNICA DEL PERÚ. Empresas en línea. [En línea] http://www.telefonica.com.pe/empresas/boletines/pdf/bolemprejulio06.pdf. [Consulta: 10 de Enero de 2007]
[32] DRUKER, F. Peter. *Los desafíos de la Gerencia para el siglo XX*!. Norma. Bogotá. 1999.

Para el autor Ribagorda Garnacho:[33] *"Vulnerabilidad es la susceptibilidad de un sistema o componente a sufrir daños por un ataque específico, o equivalentemente una debilidad del sistema de protección de un recurso que puede ser explotado por un ataque".*

Kennet Laudon[34] clasifica las amenazas más comunes que enfrentan los sistemas de información computarizados de la siguiente manera:

- Fallos de hardware
- Fallos de software
- Acciones de personal
- Penetración por terminales
- Robos de datos, servicios, equipo.
- Incendio
- Problemas eléctricos
- Errores de usuario
- Cambios de programa
- Problemas de telecomunicaciones

Estas amenazas más comunes pueden provenir de factores técnicos, organizacionales y del entorno, combinadas con decisiones administrativas deficientes.

Los adelantos en telecomunicaciones y software de computadora han intensificado esta vulnerabilidad. Gracias a las redes de telecomunicaciones es posible conectar, entre sí, sistemas de información en diferentes lugares. Así el autor Mc. Leod[35] señala que las personas que obtienen acceso no autorizado, pueden estar presentes o no en la compañía y conectarse con la red de computadoras desde una Terminal remota y causar perjuicios físicos como por ejemplo monitores dañados, discos inoperativos o teclados inhabilitados.

---

[33] RIBAGORDA GARNACHO, Arturo."*La auditoría de las redes de ordenadores"*. Documentación. Conferencia AUDISI'2000. IEE.
[34] LAUDON, Kennet y Jane LAUDON. *Sistemas de Información Gerencial*. Octava edición, Pearson Educación de México. 2004.
[35] MCLEOD JR, Raymond. *Sistemas de Información Gerencial*. Séptima edición. Prentice Hall Hispanoamericana. México, 2000.

Adicionalmente, para establecer las redes de telecomunicaciones se requieren combinaciones más complejas y diversas de hardware, software, organizacionales y de personal, lo cual genera nuevas áreas y oportunidades de penetración y manipulación. Las redes inalámbricas que usan tecnología basada en radio son incluso más vulnerables a la penetración porque las bandas de radiofrecuencia son fáciles de rastrear. La red inalámbrica que usa tecnología Wi-Fi puede ser fácil de penetrar por externos mediante computadoras portátiles, tarjetas inalámbricas, antenas externas y software de piratería informática.

Internet y la Seguridad

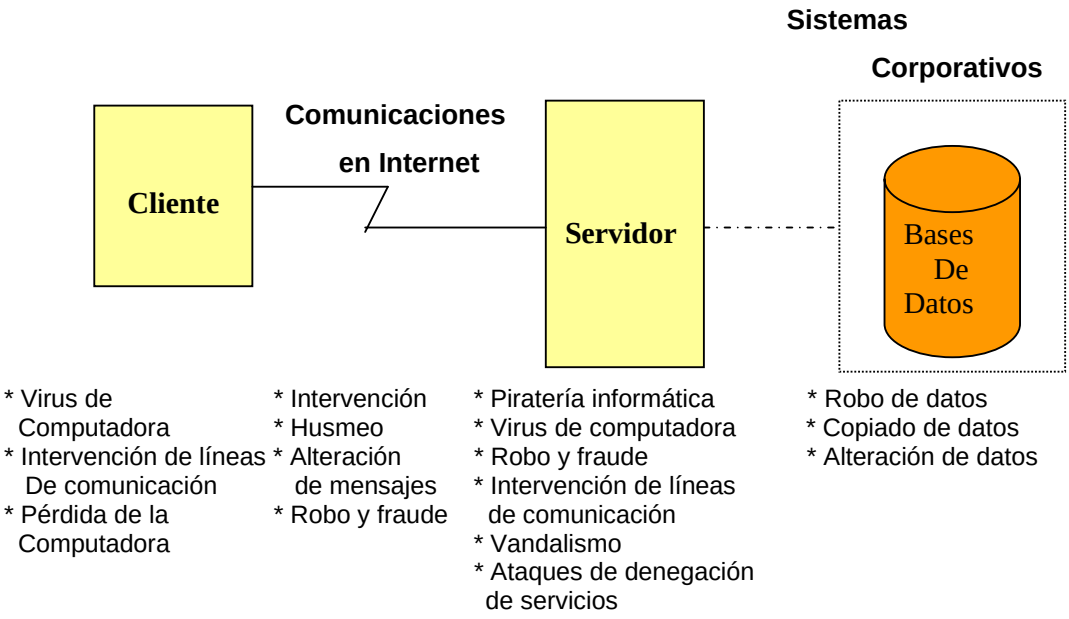
"Al Principio de Internet, todos estábamos conectados sin protección alguna. Era una época en que la masa minoritaria y, por qué no decirlo, privilegiada disfrutaba de una tecnología que no había tenido su momento de explosión. No existía la seguridad y ni tan siquiera nos importaba lo mínimo, gracias a esto, los pocos intrusos o hackers del momento realizaron conductas llamativas, pero poco a poco y conforme las empresas fueron percatándose del peligro a base de perder tiempo y dinero, se empezaron a crear sistemas de seguridad para redes, entre ellos se encuentran los famosos firewall".[36]

El cómputo de alta disponibilidad requiere una infraestructura de seguridad para el comercio electrónico y los negocios en línea. Las redes públicas grandes incluyendo a Internet, son más vulnerables porque están abiertas virtualmente a cualquiera y porque son tan grandes que cuando ocurren los abusos, pueden tener un impacto sumamente extenso. Cuando Internet pasa a formar parte de la red corporativa los sistemas de información de la organización se vuelven vulnerables a las acciones de los intrusos. La arquitectura de una aplicación basada en la Web incluye por lo común a un cliente Web, un servidor y a los sistemas de información corporativos vinculados a las bases de datos. Cada uno de estos componentes presenta retos y vulnerabilidades de seguridad, los cuales se ilustran en la figura 1.[37]

[36] ASENSIO, Gonzalo. *Seguridad en Internet*. Ediciones Nowtilus S.L. 2006.
[37] JOSHI, James y Otros. "Security Models for Web-Based Applications". Communications of the ACM 41, núm. 2 Febrero 2001.

Figura 1

Retos a la Seguridad de Internet



Fuente: *Security Models for Web-Based Applications*

También los sistemas corporativos se deben extender fuera de la organización para que los empleados que trabajan con dispositivos inalámbricos y demás dispositivos de computación móviles puedan tener acceso a ellos. Sin embargo, estos sistemas también deben estar cerrados a los hackers y otros intrusos. La nueva infraestructura de tecnología de la información requiere una nueva cultura de seguridad y una infraestructura que permitan a los negocios cruzar esta delgada línea. Las corporaciones necesitan ampliar sus políticas de seguridad con el propósito de que incluyan procedimientos para proveedores y otros socios de negocios.

Las empresas que se vinculan a Internet o transmiten la información a través de intranets y extranets requieren procedimientos de seguridad y tecnologías especiales. Los servidores de seguridad *(firewalls) sirven* para impedir que usuarios no autorizados tengan acceso a las redes privadas. Como una creciente cantidad de empresas expone sus redes al tráfico de Internet, los servidores de seguridad se están convirtiendo en una necesidad.

Oppliger[38] describe las funciones del servidor de seguridad: controla el acceso a las redes internas de la organización actuando como guardabarrera que examina las credenciales de cada usuario antes de que pueda examinar la red. El servidor de seguridad identifica nombres, direcciones de Protocolo Internet (IP), aplicaciones y otras características del tráfico entrante, y compara esta información contra las reglas de acceso que el administrador de la red ha programado en el sistema. El servidor de seguridad impide la comunicación no autorizada dentro y fuera de la red, permitiendo que la organización aplique una política de seguridad en el tráfico que fluye entre su red e Internet.

"Para crear un buen servidor de seguridad, alguien debe describir de manera bastante detallada y conservar las reglas internas que identifican a las personas, aplicaciones o direcciones que se permiten o rechazan. Los servidores de seguridad pueden desalentar, pero no impedir del todo, la penetración de la red por intrusos y deben verse como un elemento más en un plan de seguridad global. Para tratar con eficacia la seguridad de Internet, es posible que se requieran políticas corporativas y procedimientos más amplios, responsabilidades del usuario y capacitación en el conocimiento de seguridad."[39]

Dan Farmer, [40]uno de los grandes mitos del Internet y el mundo Hacker, realizó un estudio de seguridad analizando 2,203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron sitios Web con orientación al comercio, además de tomar también un conjunto de sistemas al azar para realizar comparaciones. El estudio fue realizado empleando sencillas técnicas de exploración no intrusivas (sin intento de violar el sistema, sólo explorarlo). Los problemas que detectó fueron etiquetados de maneras diferentes, rojos y amarillos. Los rojos representan problemas muy graves de seguridad y suponen que el sistema está en condiciones para que un ataque tenga éxito, son problemas de seguridad conocidos y ampliamente documentados en Internet para ser atacados. Los etiquetados con el color amarillo representan problemas menos críticos, que inicialmente no comprometen el sistema informático, pero podrían ser susceptibles de dar las primeras ideas de cómo asaltar el sistema.

---

[38] OPPLIGER, Rolf. "Internet Security. Firewalls and Beyond". Communications of de ACM 41, núm. 7 Mayo de 1997.
[39] SEGEV, Arie y Otros."Internet Security and the Case of Bank of America". Communications of the ACM 41, núm. 10. Octubre de 1998.
[40] PÉREZ AGUDIN, Justo y Otros. *La Biblia del Hacker*. Anaya Multimedia. Madrid. 2006

Las cifras que se muestran la tabla Nº 1 del estudio de D. Farmer son altamente preocupantes y nos dan una apreciación de la realidad a la que nos enfrentamos que podría ser aún más preocupante.

Tabla Nº 1

Porcentaje de vulnerabilidades por tipo de sitio

Tipo de sitio	Total de Sitios probados	% sitios vulnerables	% amarillos	% rojos
Bancos	660	68.3	32.73	35.61
Créditos	274	51.1	30.66	20.44
Sitios Federales	47	61.7	23.4	38.3
News	312	69.55	30.77	38.78
Sexo	451	66.08	40.58	25.5
Totales	1.734	64.93	33.85	31.8
Grupo al azar	469	33.05	15.78	12.27

Fuente *: http://www.trouble.org/survey*

Farmer estima que un tercio de los sitios que presentan etiquetas rojas podrían atacarse con un mínimo esfuerzo por parte de un intruso.

En la tabla Nº 2 se muestra un análisis estadístico publicada por el CERT (Computer Emergency Response Team), que sigue confirmando la falta de conciencia de las empresas e instituciones frente a los intrusos informáticos.

Tabla Nº 2

Análisis Estadístico

Año	Incidentes informados	Vulnerabilidades Informadas	Mensajes Recibidos
1989	132	0	2,868
1990	252	0	4,448
1991	406	0	9,629
1992	773	-	14,463
1993	1,334	0	21,267
1994	2,340	0	29,580
1995	2,412	171	32,084
1996	2,573	345	31,268
1997	2,134	311	39,626
1998	3,734	262	41,871
1999	9,859	417	34,612
2000	21,756	1,090	56,365
2001	52,658	2,437	118,907
2002	82,094	4,129	204,841
2003	137,529	3,784	542,754
2004 (9 meses)	-	2,683	552,320

Fuente *: CERT Internacional, http://www.cert.org/statistics*

Evaluación del riesgo

Los constructores de sistemas pueden emprender una evaluación de riesgo, determinando puntos de vulnerabilidad, la frecuencia probable de un problema y el daño potencial si el problema llegara a ocurrir. Por ejemplo, si es probable que un suceso ocurra no más de una vez en un año, con una pérdida máxima de $1,000 para la organización, no sería factible gastar $20,000 en el diseño y el mantenimiento de un control para protegerse contra un suceso. En cambio, si ese mismo suceso pudiera

ocurrir por lo menos una vez al día, con una pérdida potencial de más de $300,000 al año, gastar $100,000 en un control podría ser totalmente apropiado.

La tabla Nº 3 muestra un ejemplo de un análisis de riesgos para un sistema de procesamiento de pedidos en línea que procesa 30,000 de éstos al día. La probabilidad de que se interrumpa el suministro de electricidad en un período de un año es de 30%. La pérdida de transacciones de pedido mientras falta la electricidad podría variar entre $5,000 y $200,000 en cada ocasión, dependiendo del tiempo que esté interrumpido el procesamiento. La probabilidad de que haya un desfalco en un período de un año es de 5% y la pérdida potencial variaría entre $1,000 y $50,000 en cada caso. Los errores de usuario tienen una probabilidad de 98% de presentarse en un período de un año, con pérdidas que van desde $200 hasta $40,000 en cada ocasión. La pérdida promedio en cada caso se puede ponderar al multiplicarla por la probabilidad de que ocurra en un año, para determinar la pérdida anual esperada. Una vez evaluados los riesgos, los analistas de riesgos se concentran en los puntos de control más vulnerables y que pueden causar más pérdidas. En este caso, los controles deben enfocarse en formas de minimizar el riesgo de que falle la energía y de que los usuarios cometan errores. Incrementado la conciencia administrativa sobre toda la gama de acciones que se pueden tomar para reducir los riesgos se pueden minimizar sustancialmente las pérdidas del sistema[41].

Tabla Nº 3

Evaluación del riesgo del procesamiento de pedidos en línea

Exposición	***Probabilidad de Ocurrencia (%)***	***Rango/Promedio De pérdida ($)***	***Pérdida anual Esperada ($)***
Falla de energía	30	5,000-200,000 (102,500)	30,750
Desfalco	5	1,000-50,000 (25,500)	1275
Error de usuario	98	200-40,000 (20,100)	19,698

Fuente : *Coping with Systems Risk: Security Planning Models for Management Decision Making*

En algunas situaciones, es posible que las organizaciones no puedan conocer la probabilidad precisa de amenazas que le ocurran a sus sistemas de información, y tal vez

[41] STRAUB, Detmar y Richard WELKE. "Coping with Systems Risk: Security Planning Models for Management decision Making". MIS Quarterly 22 núm 4. Diciembre de1998.

no pueden cuantificar el impacto de tales sucesos. En esos casos, la administración puede optar por describir los riesgos y su probable impacto en forma cualitativa[42]

2.2.3 Los servicios de las universidades

La universidad constituye por sí misma un completo universo social que se proyecta más allá de la formación. La Universidad se caracteriza por brindar a sus profesores, estudiantes y trabajadores los servicios y la infraestructura necesaria, tanto técnica como humana, para el desarrollo de sus labores.

> *"Con la aparición de Internet y el avance vertiginoso de nuevas tecnologías de información y comunicación, comienzan a aparecer nuevos proyectos universitarios, que dan cuenta de nuevas formas de entender el manejo y producción de conocimiento y nuevas maneras de relación con el saber. Las nuevas tecnologías de información y comunicación han contribuido a la generación de múltiples herramientas para el uso, gestión y difusión de información, ampliando drásticamente, a la vez, la accesibilidad a dichas herramientas, a través de medios digitales de transmisión. Todo ello sumado al impacto cultural que ha significado para la humanidad el mayor acceso a la publicación de conocimientos locales y aplicados."* [43]

Por otro parte el autor Espinoza[44] señala que la nueva universidad se caracteriza porque tiene capacidad para generar recursos propios a través de la producción de bienes y servicios, alianzas o convenios con el sector empresarial, administración rentable de la infraestructura universitaria, etc. Igualmente la nueva universidad se caracteriza por la existencia de un sistema de administración de las finanzas (ingresos e inversiones) sujeto a planes y programas así como a razones técnicas y éticas y a las características de cada universidad con plena autonomía pero sujeto a las auditorías

---

[42] RAINER, Rex Kelley y Otros. "Risk Analysis for Information Technology". Journal of Management Information Systems 8, núm 1. 1991.

[43] ENCICLOPEDIA WIKIPEDIA. [En línea]. http://es.wikipedia.org/wiki/Universidad. [Consulta: 20 de Setiembre 2006]

[44] ESPINOZA Herrera, Nemesio. *Gerencia Universitaria. Universidad Peruana y Tercer Milenio*. San Marcos. Lima. 2000.

contables tanto internas como externas así como de otros mecanismos técnicos eficaces de control financiero.

Mencionaremos algunos de los servicios que brindan las Universidades:

Servicios académicos y Administrativos

- Matrícula
- Admisión y Registros
- Tesorería
- Grados y Títulos
- Bibliotecas
- Becas para alumnos y docentes

Servicios Tecnológicos

- Soporte a los sistemas de información
- Correo Electrónico
- Laboratorio de Microcomputadoras

Otros Servicios

- Bienestar Universitario
- Oficina de Apoyo Financiero
- Servicio de Salud
- Centro cultural y Deportes
- Centro de Idiomas

2.2.3.1 Servicios Críticos de las Universidades

Consideramos servicios críticos de las Universidades a los servicios tales como: Matrícula, Admisión y Registros, Grados y Títulos, Contabilidad y Tesorería e Informática, porque recopilan información que puede ser mucho más completa, y más confidencial, que aquella del mundo corporativo, como por ejemplo tienen Registro de postulantes, Registros de alumnos como sus notas de cursos, certificados de estudios, documentación de Grados y Títulos, bases de datos financieros y presupuestal, registro de direcciones de correo electrónico de alumnos y docentes, etc. Estos servicios basados

en sistemas de información están en constante amenaza de intrusos tanto internos como externos y es necesario reevaluar y buscar medidas de seguridad más estrictas para proteger la información confidencial de las instituciones educativas. A continuación mencionamos algunos antecedentes de incidentes de seguridad ocurridos en varias instituciones educativas y que para minimizar los riesgos de seguridad de sus recursos de información han optado por usar normas y políticas de seguridad y así mejorar sus servicios con calidad y seguridad para los alumnos, docentes y los mismos trabajadores:

> "Hasta hace poco, era común que las universidades usaran los números de la Seguridad Social o Cedula de Identidad (u otro número de identificación personal) no solamente para las tarjetas de identificación, sino también para las tarjetas de la biblioteca, nombramientos públicos por grado de escalafón, listas de estudiantes, inscripción a los cursos, listados de correo electrónico de los estudiantes y para muchas otras actividades y comunicaciones del campus. Esta práctica se está reconsiderando a la luz de los recientes ataques de los hackers y de otros incidentes de gran magnitud en que se robaron de las instituciones académicas los registros almacenados en la computadora en varias universidades de Estados Unidos. Un incidente ocurrió en la Universidad de Texas en el año 2005 donde los nombres y números de la Seguridad Social de 55.000 estudiantes, ex alumnos, cuerpo docente y personal se vieron comprometidos por un hacker, que también era estudiante de la universidad . Otro caso ocurrió en la Universidad de Washington Central En el año 2000, un profesor de filosofía fue condenado a seis meses de cárcel por fraude con tarjeta de crédito como resultado del robo de los números de Seguridad Social de los estudiantes, perpetrado desde los equipos de la universidad. "[45]

En la Universidad Carlos III de Madrid[46] era imposible asignar una computadora a cada alumno, tanto por cuestiones económicas como de logística y administración. La ausencia de un sistema de identificación más fiable suponía distintos problemas, principalmente tres: En primer lugar, no se tenía un registro de sesiones, por lo que no

[45] SYMANTEC CORPORATION. "Universidades abordan el problema del robo de identidad". [En línea]: http://www.symantec.com/region/mx/enterprisesecurity/content/government/LAM_3583.html [Consulta: 15 Agosto de 2006]

[46] UNIVERSIDAD CARLOS III DE MADRID**.** La innovación al servicio del alumno. [En línea] http://www.microsoft.com/spain/enterprise/casestudies/cs_uni_carlosiii01.aspx. [Consulta: 15 Agosto de 2006]

se podía conocer la identidad del usuario. Ese anonimato era aprovechado por algunos para ejecutar acciones que comprometían la seguridad de las máquinas. En segundo lugar, muchas personas ajenas a la comunidad universitaria se acercaban a las aulas para navegar por Internet, razón por la cual los alumnos veían limitado el parque de computadoras. Y en tercer lugar, antes de los exámenes y coincidiendo con la entrega de trabajos y prácticas, se recibía muchas quejas por parte del alumnado en el sentido de que algunos compañeros monopolizaban los equipos. Todo esto los llevó a la necesidad de desarrollar e implantar un sistema que les ayudara a disminuir las incidencias de seguridad, optimizar la gestión de las computadoras y mejorar el servicio.

A continuación mencionamos los beneficios obtenidos:

- Disminución de incidencias de seguridad**.** Las incidencias de seguridad relacionadas con el uso de los PCs por parte de los estudiantes han disminuido considerablemente, por no decir que prácticamente son inexistentes. Esta es la gran ventaja de saber quién está en cada puesto de trabajo.
- Optimización de la gestión de PCs**.** Desde el punto de vista de la eficiencia operacional, la solución permite monitorizar y administrar remotamente el aula en cada momento, lo que evita el tener que controlar individualmente cada puesto.
- Mejora del servicio. El sistema tiene un módulo de estadísticas que ayuda a la Universidad a identificar posibles necesidades en relación con los puestos de trabajo por alumno (qué aulas son las más utilizadas, en qué horarios, cuántos alumnos han accedido a ellas). El sistema también dispone de una herramienta que permite asignar un porcentaje de uso diario a cada estudiante.

La Universidad Autónoma de México (UNAM)[47] ha sufrido diversos ataques electrónicos, uno de los más importantes se registró en 1993 contra la supercomputadora CRAY YMP e involucró otros equipos, y que tras una exhaustiva investigación, se determinó que el ataque había se había originado dentro de la misma UNAM en el Instituto de Ciencias Nucleares. A raíz de este incidente se fundó el Equipo de Seguridad en Cómputo (ESC) de la UNAM, para difundir la cultura de seguridad en cómputo y ayudar a la comunidad universitaria ante cualquier eventualidad. Actualmente la UNAM-

[47]RODRIGUEZ HERNANDEZ, Eduardo. *Arquitectura de Seguridad de la Red Inalámbrica Universitaria*. [En línea]. http://www.astralix.com/papers/riu-titulacion-espina.pdf. [Consultado: 10 de Diciembre de 2006]

CERT tiene un Equipo de Respuesta a Incidentes, que es un equipo de especialistas de seguridad en cómputo que atiende a instituciones de cualquier tipo que han sido víctimas de algún ataque tanto en sus sistemas de cómputo como en sus sitios de Internet.

CAPITULO III

LA ENCUESTA Y ANALISIS DE RESULTADOS

3.1 ANALISIS E INTERPRETACION DE RESULTADOS

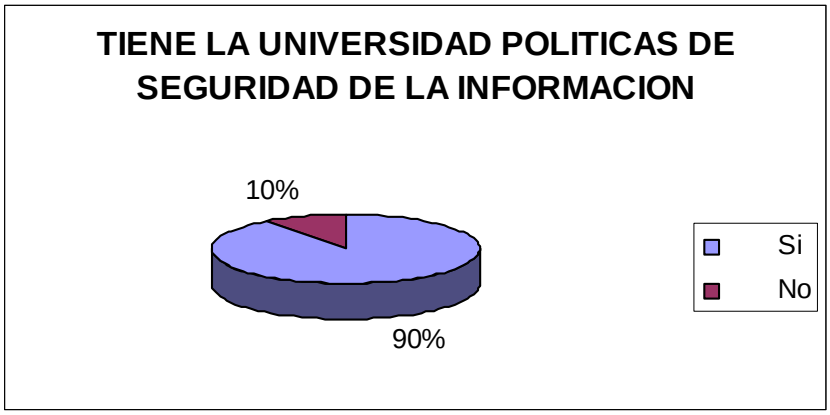
3.1.1 Universidad Nacional Mayor de San Marcos

Cuadro Nº 01

¿En la Universidad donde labora tienen políticas de seguridad de la información?

Opción	Frecuencia
Si	9
No	1

Gráfico Nº 01



Análisis Interpretativo

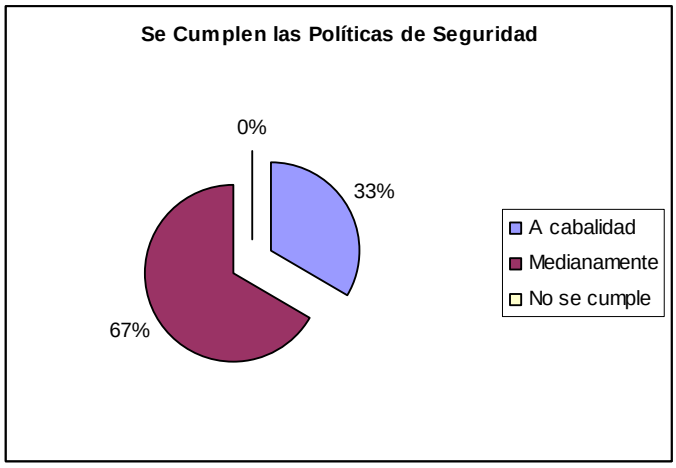
El 90% de los encuestados respondió que la Universidad cuenta con políticas de seguridad de la información, un 10% opina lo contrario.

Cuadro Nº 02

¿Si en la Pregunta 1 respondió si, se cumplen o se llevan a la práctica estas políticas?

Se cumplen las políticas de Seguridad	Frecuencia	%
A cabalidad	3	33
Medianamente	6	67
No se cumple	0	0
Total	9	100

Gráfico Nº 02



Análisis Interpretativo

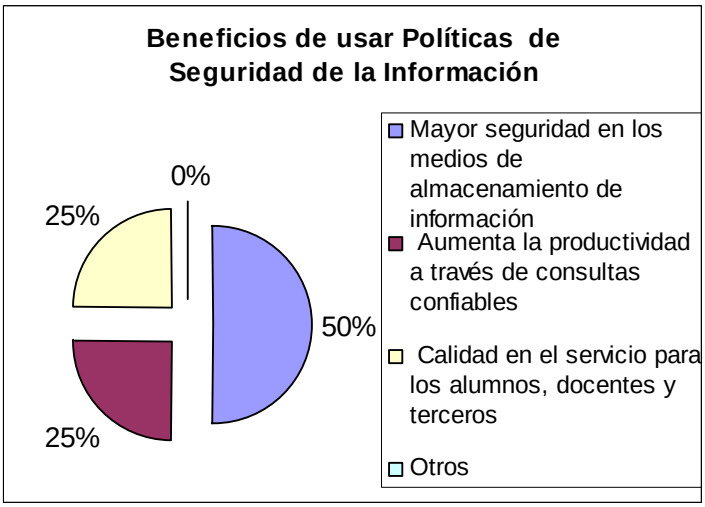
Del total de personas que respondió que en la Universidad tienen políticas de seguridad, un 33% opina que si se cumplen a cabalidad y que un 67% lo hace medianamente, es decir no siempre se toma en cuenta estas políticas como mejores prácticas de seguridad. Por los resultados obtenidos, podemos concluir que la Universidad no cuenta con un área que desarrolle políticas de seguridad de la información y muchos que respondieron que sí lo hicieron para dar la apariencia de cumplir con estos requisitos.

Cuadro Nº 03

¿Elija que beneficios se presentan cuando la Universidad cuenta con Políticas de Seguridad la información?. Marcar una o más opciones.

Opciones	Frecuencia	%
Mayor seguridad en los medios de almacenamiento de información	8	50
Aumenta la productividad a través de consultas confiables	4	25
Calidad en el servicio para los alumnos, docentes y terceros	4	25
Otros	0	0
Total	**16**	**100**

Gráfico Nº 03



Análisis Interpretativo

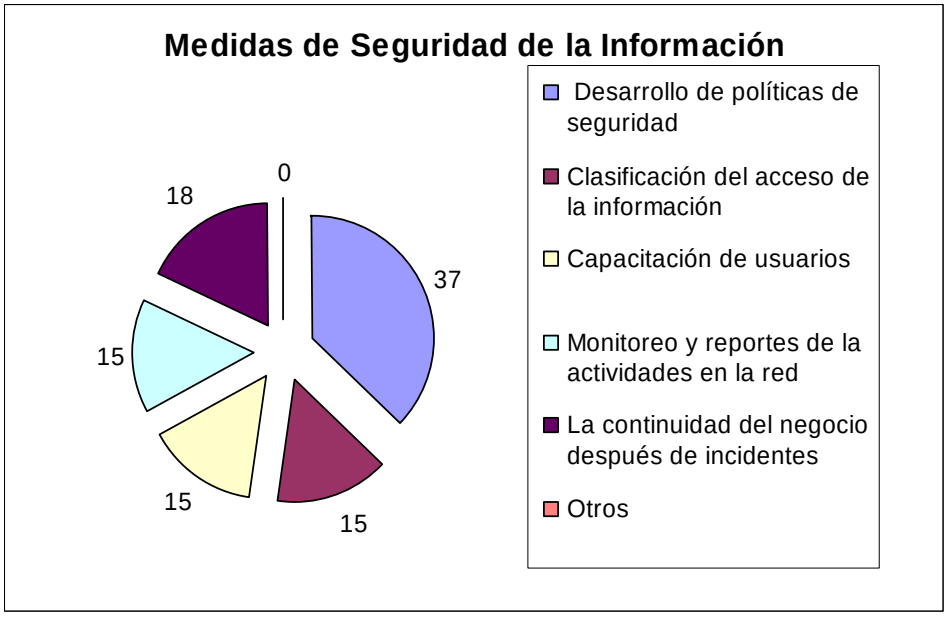
Del total de respuestas marcadas el 50% considera que la mayor seguridad de los medios de almacenamiento de información es uno de los beneficios de usar políticas de seguridad de la información, un 25% apuesta por la calidad en el servicio a los alumnos y docentes y el otro 25% consideran que aumenta la productividad a través de consultas confiables.

Cuadro Nº 04

¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la información?. Marcar una o más opciones.

Medidas en la Gestión de seguridad de la información	Frecuencia	%
Desarrollo de políticas de seguridad	10	37
Clasificación del acceso de la información	4	15
Capacitación de usuarios	4	15
Monitoreo y reportes de la actividades en la red	4	15
La continuidad del negocio después de incidentes	5	18
Otros	0	0
Total	**27**	**100**

Gráfico Nº 04



Análisis Interpretativo

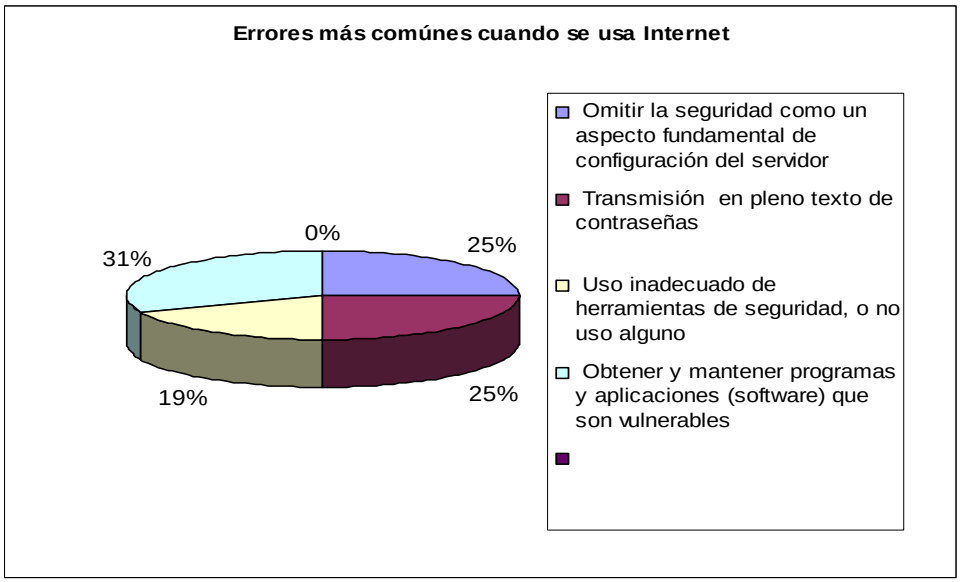
Sobre qué medidas de seguridad de la información son las más prioritarias, un 37% considera el desarrollo de políticas de seguridad, un 18% opina que la continuidad del negocio es muy importante y en un 15% consideran a la capacitación de usuarios, clasificación y acceso a la información y monitoreo de las actividades de la red informática de la UNMSM.

Cuadro Nº 05

¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico? Marcar una o más opciones.

Errores más comunes cuando se usa Internet y el correo electrónico	Frecuencia	%
Omitir la seguridad como un aspecto fundamental de configuración del Servidor	4	25
Transmisión en pleno texto de contraseñas	4	25
Uso inadecuado de herramientas de seguridad, o no uso alguno	3	19
Obtener y mantener programas y aplicaciones (software) que son vulnerables	5	31
Otros	0	0
Total	**16**	**100**

Gráfico Nº 05



Análisis Interpretativo

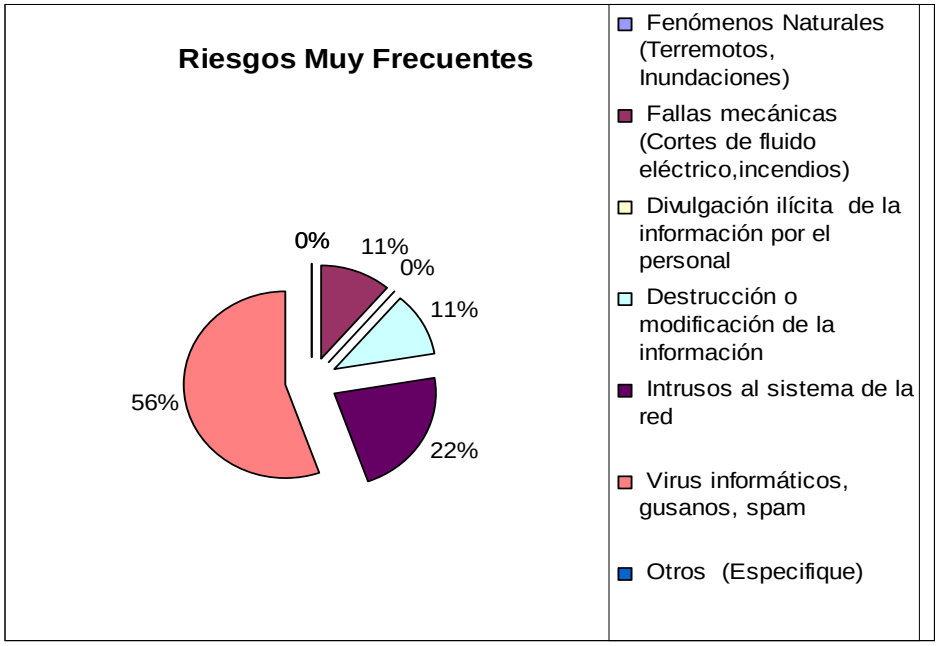
Podemos apreciar que todos los errores mencionados son muy comunes cuando se usa Internet, pero sobresale con un 31% el obtener y mantener programas que son vulnerables. Le siguen como errores más frecuentes el omitir la seguridad al momento de configurar el servidor y la transmisión en pleno texto de contraseñas con un 25% y finalmente otro error común es el uso inadecuado de herramientas de seguridad.

Cuadro Nº 06

¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?
MF = Muy Frecuentes RF = Regularmente frecuentes PF = Poco frecuentes

Riesgos	MF	%	RF	%	PF	%
Fenómenos Naturales (Terremotos, Inundaciones)	0	0	0	0	10	38
Fallas mecánicas (Cortes de fluido eléctrico, incendios)	1	11	5	20	4	15
Divulgación ilícita de la información por el personal	0	0	7	28	3	12
Destrucción o modificación de la información	1	11	2	8	7	27
Intrusos al sistema de la red	2	22	6	24	2	8
Virus informáticos, gusanos, spam	5	56	5	20	0	0
Otros (Especifique)	0	0	0	0	0	0
Total	**9**	**100**	**25**	**100**	**26**	**100**

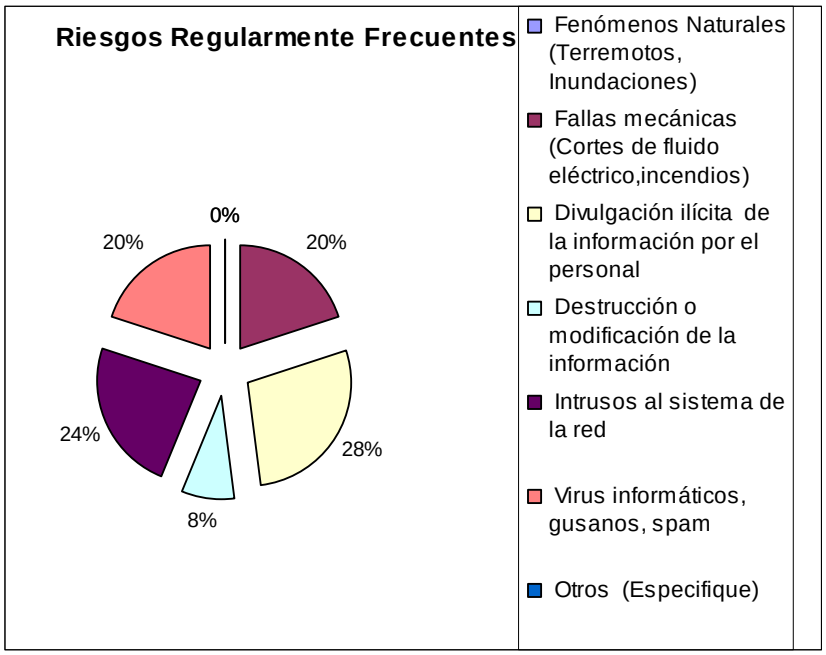
Gráfico Nº 06.1



Análisis Interpretativo

Según el gráfico, los riesgos más frecuentes que se presentan en la UNMSM son “los virus informáticos, gusanos y spam “ con un 56%, en segundo lugar están “los intrusos al sistema de la red” con un 22% y el tercer lugar lo comparten “las fallas mecánicas” como los cortes de fluido eléctrico y “la destrucción y/o modificación de la información” con un 11%.

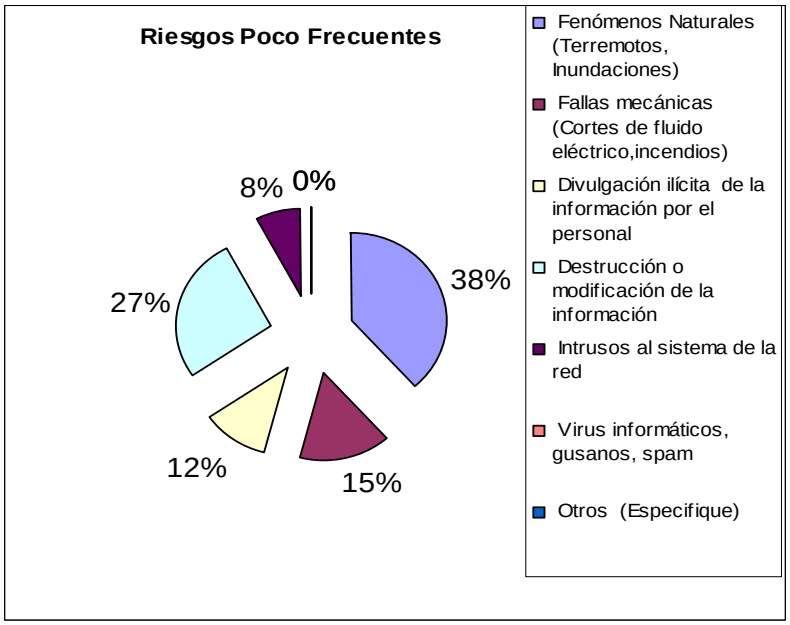
Gráfico Nº 06.2



Análisis Interpretativo

Los riesgos regularmente frecuentes se presentan en su mayoría por: divulgación ilícita de la información (28%), por los intrusos al sistema de la red (24%), por los cortes de fluido eléctrico (20%), por los virus informáticos (20%) y una minoría considera como riesgo regularmente frecuente la destrucción o modificación de la información por parte del personal (8%).

Gráfico Nº 06.3



Análisis Interpretativo

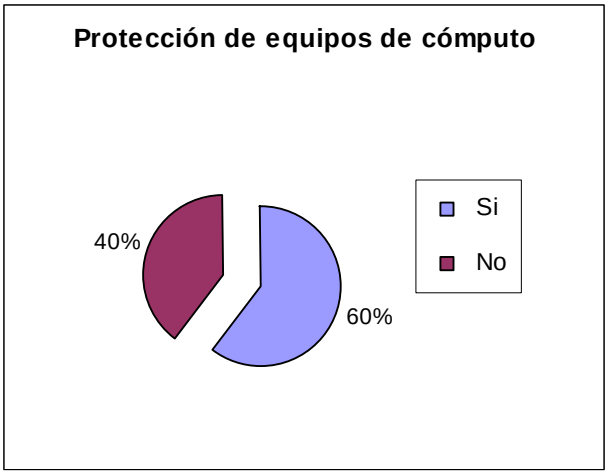
Los riesgos poco frecuentes se presentan ocasionalmente por fenómenos naturales como terremotos o inundaciones (38%), por la destrucción de la información por parte del personal (27%) y en algunos casos por los cortes de fluido eléctrico (15%).

Cuadro Nº 07

¿Sus equipos de cómputo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?

Protección de equipos cómputo	Frecuencia	%
Si	6	60
No	4	40
Total	**10**	**100**

Gráfico Nº 07



Análisis Interpretativo

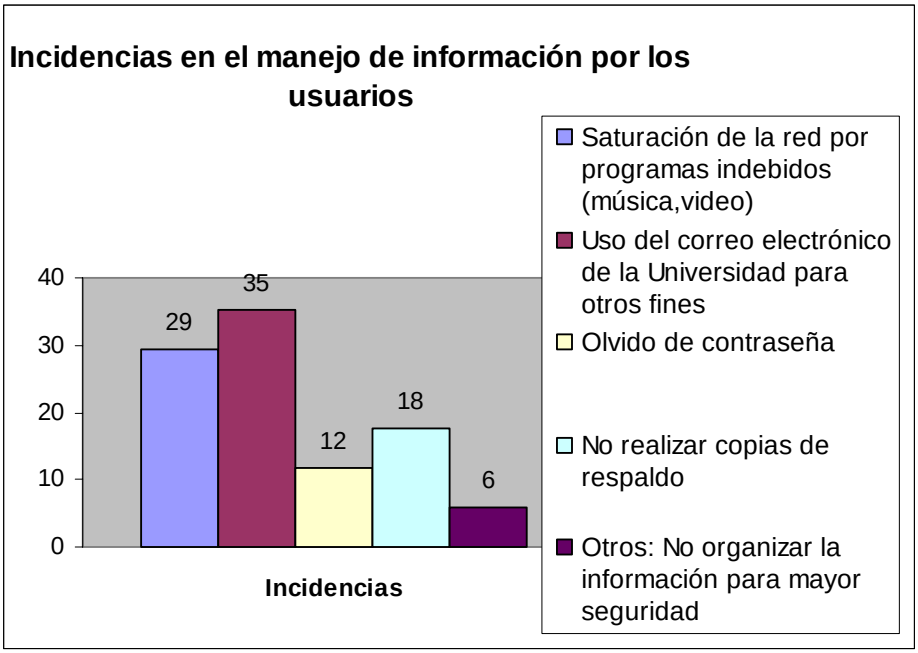
Según el gráfico del total de encuestados un 60% cuenta con equipos en sus oficinas para protegerse ante cortes de energía eléctrica y hay un considerable 40% que no tienen estos equipos de protección.

Cuadro Nº 08

Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

Incidencias que se dan con más frecuencia	Frecuencia	%
Saturación de la red por programas indebidos (música, video)	5	29
Uso del correo electrónico de la Universidad para otros fines	6	35
Olvido de contraseña	2	12
No realizar copias de respaldo	3	18
Otros: No organizar la información para mayor seguridad	1	6
Total	17	100

Gráfico Nº 08



Análisis Interpretativo

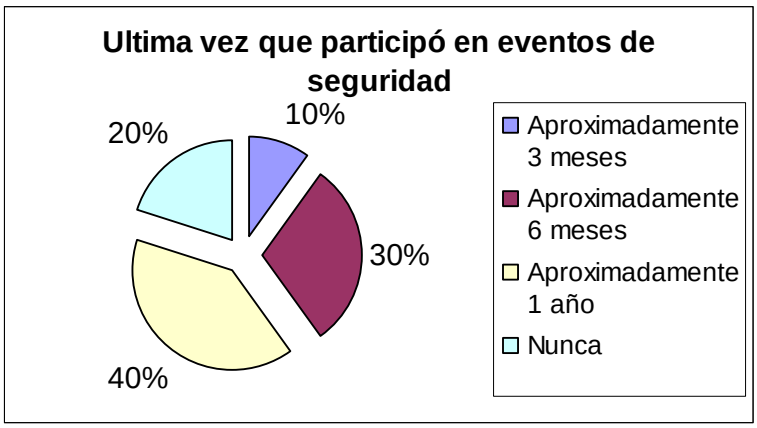
Del total de respuestas recogidas las incidencias más frecuentes son: el uso del correo electrónico de la Universidad para fines personales con 35% , la saturación de la red e Internet por programas indebidos (29%); y menos frecuentes pero que tampoco dejan de ser preocupantes son: los usuarios que no realizan copias de seguridad (18%) y el olvido de sus contraseñas (12%) y en la opción otros un 6% de respuestas coincidieron que existen usuarios que no organizan sus archivos, lo que genera también problemas de seguridad.

Cuadro Nº 09

¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

Ultima vez que participó a eventos	Frecuencia	%
Aproximadamente 3 meses	1	10
Aproximadamente 6 meses	3	30
Aproximadamente 1 año	4	40
Nunca	2	20
Total	10	100

Gráfico Nº 09



Análisis Interpretativo

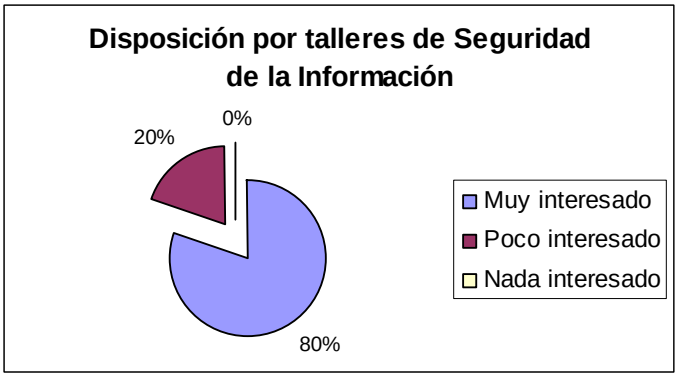
El 20% del personal de TIC de la UNMSM nunca ha asistido a eventos o talleres de seguridad de la información pero también hay personas que concientes del problema de seguridad han asistido de alguna manera a talleres o seminarios de seguridad de información, así un 40% ha asistido aproximadamente hace 1 año, un 30% ha participado aproximadamente hace 6 meses y un 10% ha asistido aproximadamente hace 3 meses.

Cuadro Nº 10

¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

Disposición a talleres de Capacitación	Frecuencia	%
Muy interesado	8	80
Poco interesado	2	20
Nada interesado	0	0
Total	**10**	**100**

Gráfico Nº 10



Análisis Interpretativo

Del personal encuestado un 80% está muy interesado si se realizan programas y talleres de capacitación de seguridad de la información, existe un 20% que está poco interesado debido a que no consideran a la seguridad como una prioridad dentro de la universidad. Lo positivo es que no hay ningún personal que esté ajeno a la capacitación de seguridad.

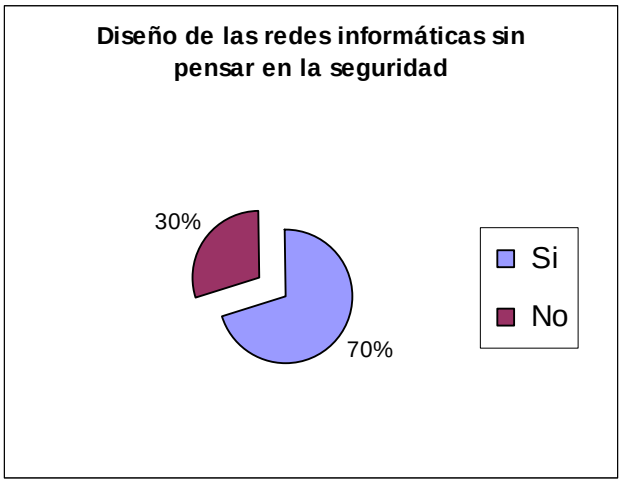
Cuadro Nº 11

¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad . Porqué?

	Frecuencia	%
Si	7	70
No	3	30
Total	100	100

	Razones
Si	• No había Internet y por ende no había riesgos a la información • La Universidad como centro de investigación no debe tener restricciones en el acceso a la información
No	• Se diseñó pensando en la seguridad de acuerdo a la tecnología de ese tiempo

Gráfico Nº 11



Análisis Interpretativo

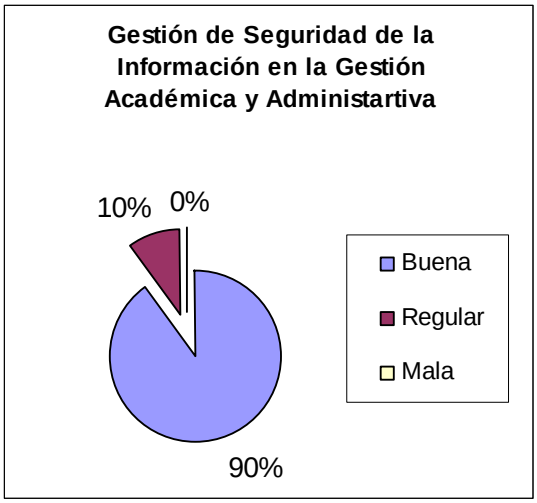
Sobre si las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad un 70% considera que sí, y las razones se han consolidado en el cuadro anterior. Por otra parte un 30% opina lo contrario.

Cuadro Nº 12

¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son: matrícula de alumnos, admisión y registros, tesorería, y trámites documentarios?

Gestión de la Seguridad en la Gestión Académica y Administrativa	Frecuencia	%
Buena	9	90
Regular	1	10
Mala	0	0
Total	**10**	**100**

Gráfico Nº 12



Análisis Interpretativo

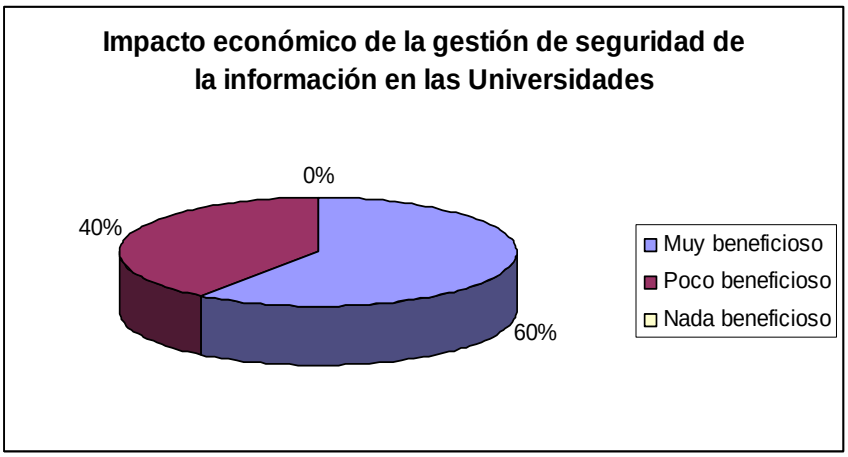
Del total del personal de TIC un 90% considera que la gestión de seguridad de la información en la gestión académica y administrativa es buena, sólo un 10% opina que la gestión es regular pues han sido partícipes de diferentes problemas de seguridad y nadie considera que la gestión es mala.

Cuadro Nº 13

¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?

Impacto económico	Frecuencia	%
Muy beneficioso	6	60
Poco beneficioso	0	0
Nada beneficioso	4	40
Total	**10**	**100**

Gráfico Nº 13



Análisis Interpretativo

Con respecto al impacto económico de implementar un plan de gestión de seguridad de la información en la gestión integral de la Universidad las apreciaciones se encuentran divididas pues si bien hay un 60% que lo considera muy beneficioso existe un 40% que piensa que es poco beneficioso. Por otro lado no hay ningún personal que opina que el impacto económico no es beneficioso.

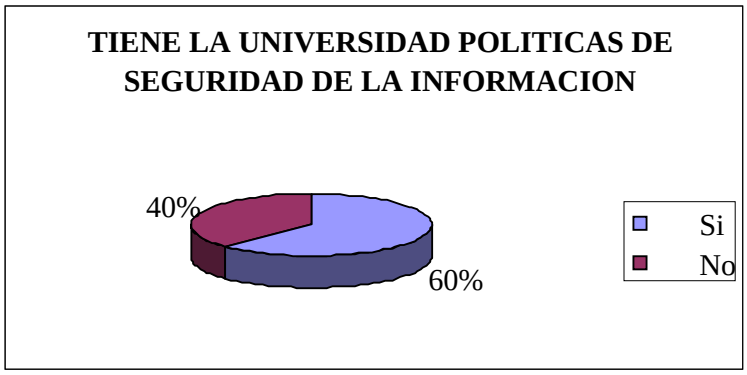
3.1.2 Universidad Nacional Federico Villarreal

Cuadro Nº 14

¿En la Universidad donde labora tiene políticas de seguridad de la información?

Opción	Frecuencia
Si	6
No	4

Gráfico Nº 14



Análisis Interpretativo

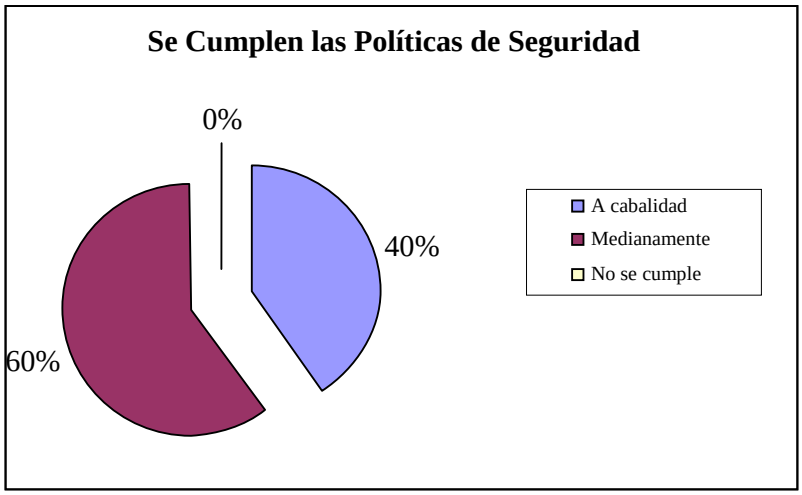
El 60% de los encuestados afirma que la Universidad tiene políticas de seguridad de la información pero hay un grupo de 40% que opina lo contrario pues nunca las autoridades lo han hecho de conocimiento o simplemente no las hay.

Cuadro Nº 15

¿Si en la Pregunta 1 respondió si, Se cumplen o se llevan a la práctica estas políticas?

Se cumplen las políticas de Seguridad	Frecuencia	%
A cabalidad	2	40
Medianamente	4	60
No se cumple	0	0
Total	6	100

Gráfico Nº 15



Análisis Interpretativo

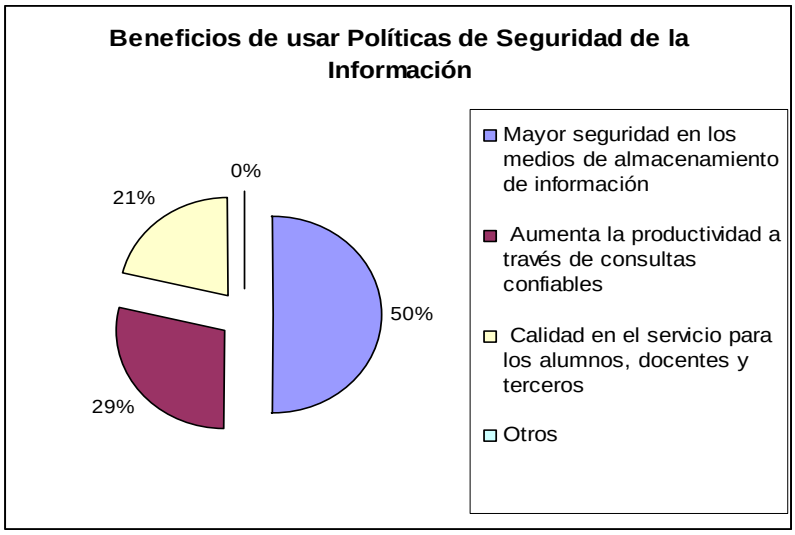
De total de personas que respondió que en la Universidad tienen políticas de seguridad un 40% opina que se cumplen a cabalidad mientras que un 60% lo hace medianamente, es decir no siempre toma en cuenta estas políticas como mejores prácticas de seguridad.

Cuadro Nº 16

¿Elija que beneficios se presentan cuando la Universidad cuenta con Políticas de Seguridad la información?. Marcar una o más opciones.

Opciones	Frecuencia	%
Mayor seguridad en los medios de almacenamiento de información	7	50
Aumenta la productividad a través de consultas confiables	4	29
Calidad en el servicio para los alumnos, docentes y terceros	3	21
Otros	0	0
Total	**14**	**100**

Gráfico Nº 16



Análisis Interpretativo

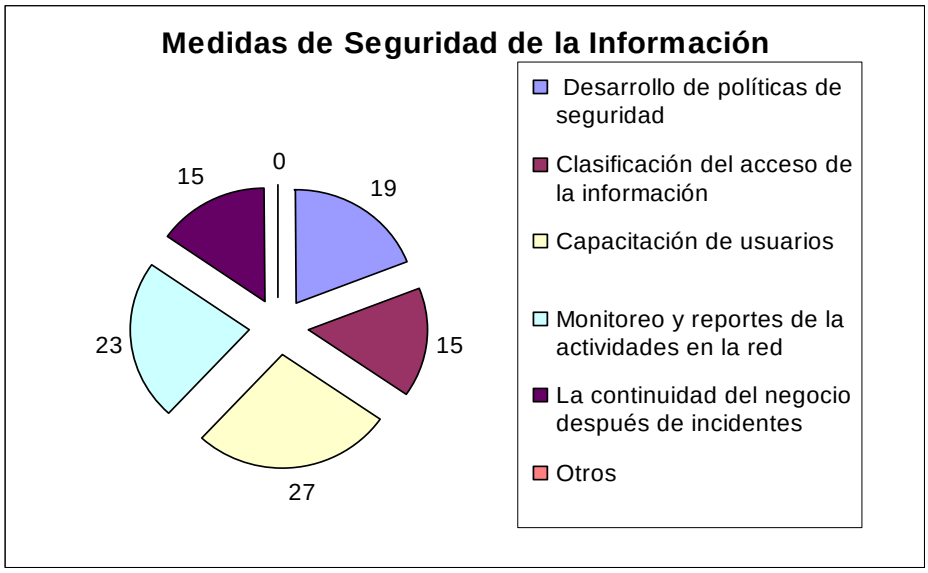
Del total de respuestas marcadas el 50% considera que la mayor seguridad de los medios de almacenamiento de información es uno de los beneficios de usar políticas de seguridad de la información, un 29% considera que aumenta la productividad a través de consultas confiables, un 21% apuesta por la calidad en el servicio a los alumnos y docentes, y un 0% no encuentra otro beneficio de los ya mencionados.
Los medios de almacenamiento deben estar protegidos porque guardan el activo más valioso de la Institución, y físicamente el "respaldo" debe estar fuera de la institución como una medida preventiva, por otra parte al existir seguridad las consultas serán más productivas a la hora de tomar decisiones importantes. Finalmente el tener políticas de seguridad beneficia con una mejor calidad en el servicio a los alumnos, docentes y terceros cuando acceden a aplicaciones por la red y el Internet.

Cuadro Nº 17

¿Cuáles de estas medidas de seguridad de la información son las más prioritarias para Usted?. Marcar una o más opciones.

Medidas de Seguridad de la Información	Frecuencia	%
Desarrollo de políticas de seguridad	5	19
Clasificación del acceso de la información	4	15
Capacitación de usuarios	7	27
Monitoreo y reportes de la actividades en la red	6	23
La continuidad del negocio después de incidentes	4	15
Otros	0	0
Total	**26**	**100**

Gráfico Nº 17



Análisis Interpretativo

Del total de respuestas obtenidas sobre qué medidas de seguridad consideran las más prioritarias un 23% considera la capacitación de los usuarios, en segundo lugar se encuentra el monitoreo y reportes de las actividades en la red con un 23% , en tercer lugar está “proteger los servidores y su información” con un 19% y “la clasificación de acceso a la información” y “La continuidad del negocio después de un incidente” con un 15% ambos.

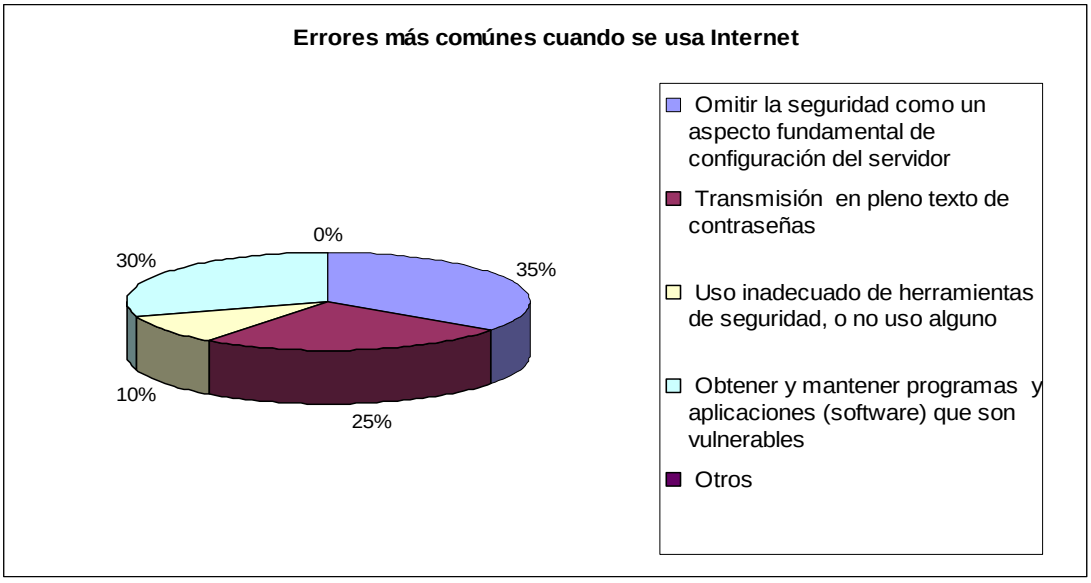
Los resultados nos muestran que la capacitación a los usuarios es de vital importancia porque el mayor número de riesgos que se presentan está relacionados con ellos pues no tiene una cultura de seguridad y lo que se trata es de sensibilizarlos con talleres de capacitación.

Cuadro Nº 18

¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico? Marcar una o más opciones.

Errores más comunes cuando se usa el correo electrónico y el Internet	Frecuencia	%
Omitir la seguridad como un aspecto fundamental de configuración del Servidor	7	35
Transmisión en pleno texto de contraseñas	5	25
Uso inadecuado de herramientas de seguridad, o no uso alguno	2	10
Obtener y mantener programas y aplicaciones (software) que son vulnerables	6	30
Otros	0	0
Total	**20**	**100**

Gráfico Nº 18



Análisis Interpretativo

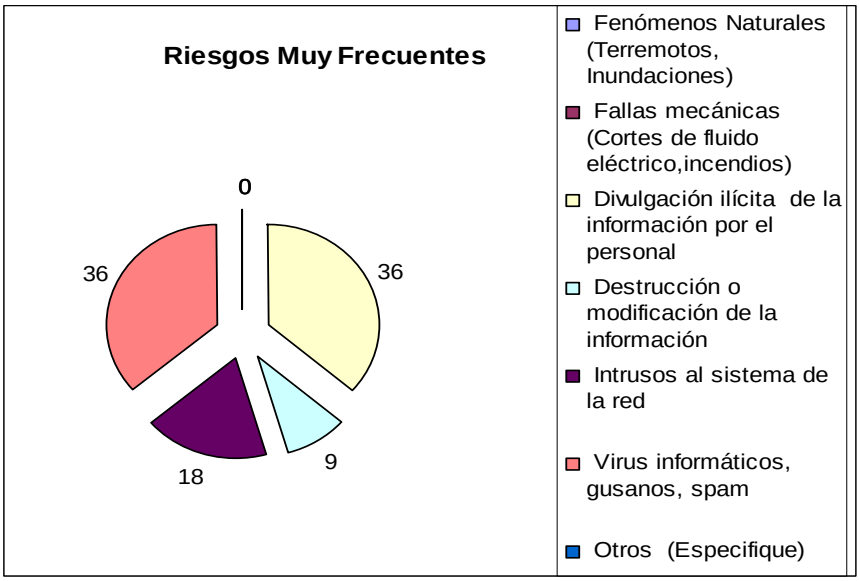
Podemos apreciar que todos los errores mencionados son muy comunes cuando se usa Internet, pero sobresale con más porcentaje "el omitir la seguridad al momento de configurar el servidor " con un 35% porque es un riesgo muy alto y el servidor puede ser vulnerable ante ataques de intrusos, "el mantener software vulnerable" también es un error común con un 30%. El descuido y la falta de cultura de seguridad de los usuarios hacen que otras personas conozcan su clave de acceso (25%) y finalmente el uso de herramientas de seguridad inapropiadas que puede ser sin licencia o que no se adaptan a las necesidades de la institución (10%).

Cuadro Nº 19

¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?
MF = Muy Frecuente RF = Regularmente frecuente PF = Poco frecuente

Riesgos	MF	%	RF	%	PF	%
Fenómenos Naturales (Terremotos, Inundaciones)	0	0	3	20	4	20
Fallas mecánicas (Cortes de fluido eléctrico, incendios)	0	0	2	13	5	25
Divulgación ilícita de la información por el personal	4	36	2	13	2	10
Destrucción o modificación de la información	1	9	3	20	3	15
Intrusos al sistema de la red	2	18	3	20	2	10
Virus informáticos, gusanos, spam	4	36	2	13	2	10
Otros (Especifique)	0	0	0	0	2	10
Total	**11**	**100**	**15**	**100**	**20**	**100**

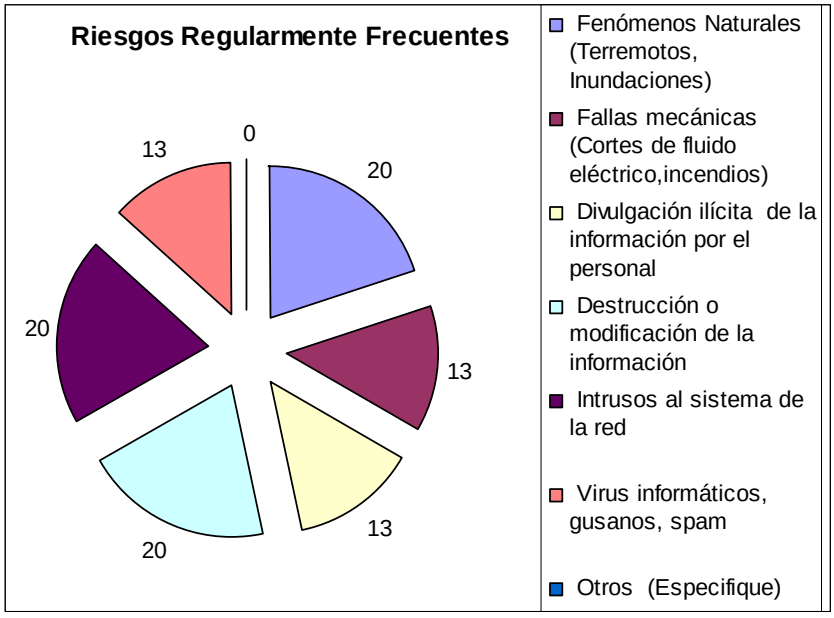
Gráfico Nº 19.1



Análisis Interpretativo

Según el gráfico, los riesgos más frecuentes que se presentan en la Universidad Nacional Federico Villarreal son los virus informáticos, gusanos y spam y la divulgación ilícita de información por el personal con un 36%, en segundo lugar están “los intrusos al sistema de la red” con un 27% , en tercer lugar se encuentra la destrucción y/o modificación de la información con un 9%. No consideran muy frecuentes los riesgos de fenómenos naturales y fallas mecánicas.

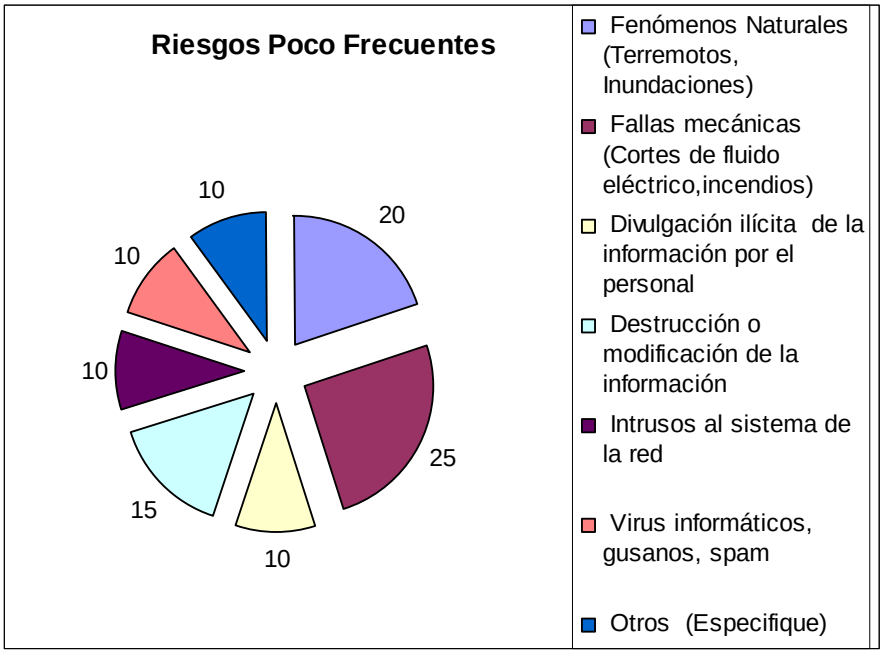
Gráfico Nº 19.2



Análisis Interpretativo

Los riesgos regularmente frecuentes se presentan en 2 grupos : el primero en su mayoría por las fallas naturales como terremotos (20%), modificación de la información (20%) y los intrusos a la red (20%) y el segundo grupo en menor proporción es por virus informáticos (13%) , divulgación ilícita de la información por el personal (13%) y fallas mecánicas (13%).

Gráfico Nº 19.3



Análisis Interpretativo

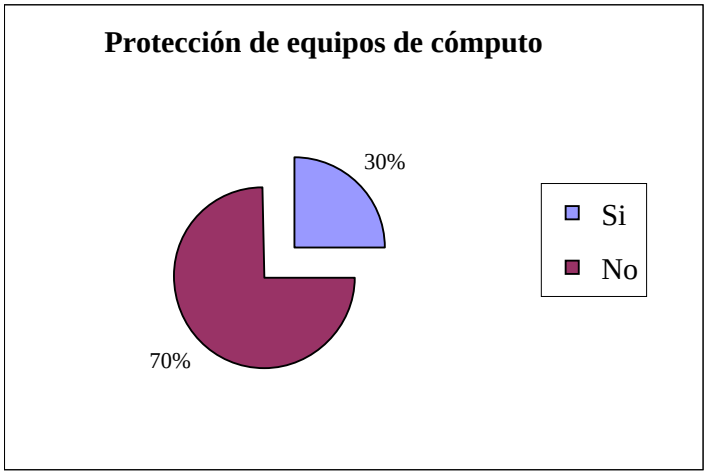
Los riesgos poco frecuentes en su mayoría se presentan por fenómenos naturales (20%) y fallas mecánicas (25%) y en su minoría se presenta por destrucción de la información por el personal (15%) , intrusos al sistema de la red (10%) y virus informáticos (10%).

Cuadro Nº 20

¿Sus equipos de cómputo en sus oficinas tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?

Protección de equipos cómputo	Frecuencia	%
Si	3	30
No	7	70
Total	**10**	**100**

Gráfico Nº 20



Análisis Interpretativo

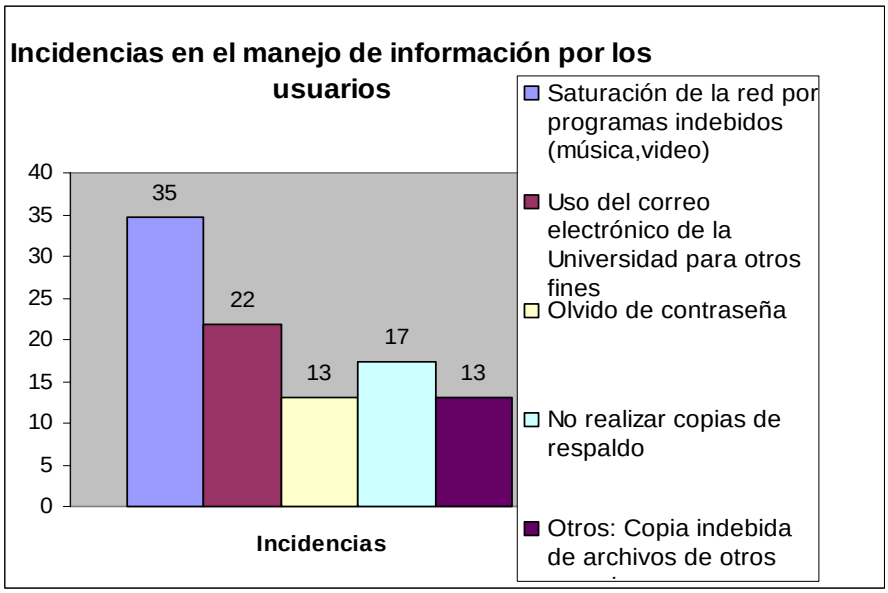
Según el gráfico la situación es preocupante porque sólo un 30% de los encuestados afirmó que cuenta con equipos electrónicos para salvaguardar la información mientras que un 70% no tienen equipos en sus oficinas para protegerse ante cortes de energía eléctrica y otra eventualidad.

Cuadro Nº 21

¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

Incidencias que se dan con más frecuencia	Frecuencia	%
Saturación de la red por programas indebidos (música, video)	8	35
Uso del correo electrónico de la Universidad para otros fines	5	22
Olvido de contraseña	3	13
No realizar copias de respaldo	4	17
Otros: Copia indebida de archivos de otros usuarios	3	13
Total	23	100

Gráfico Nº 21



Análisis Interpretativo

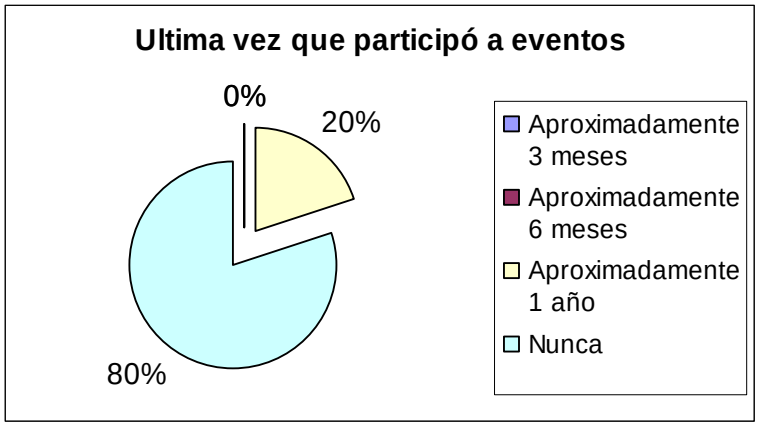
Del total de respuestas recogidas una de las incidencias más frecuentes es la saturación de la red e Internet por programas indebidos (35%), el uso del correo de la Universidad para fines personales con 22%. Los usuarios no realizan copias de seguridad de su información y corren un gran riesgo (17%), también es preocupante el olvido de contraseñas (13%) y en la opción otros un 13% de respuestas coincidieron que “existen usuarios que dedican su tiempo a copiar archivos ajenos.

Cuadro Nº 22

¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

Ultima vez que participó a eventos de seguridad de la información	Frecuencia	%
Aproximadamente 3 meses	0	0
Aproximadamente 6 meses	0	0
Aproximadamente 1 año	2	20
Nunca	8	80
Total	10	100

Gráfico Nº 22



Análisis Interpretativo

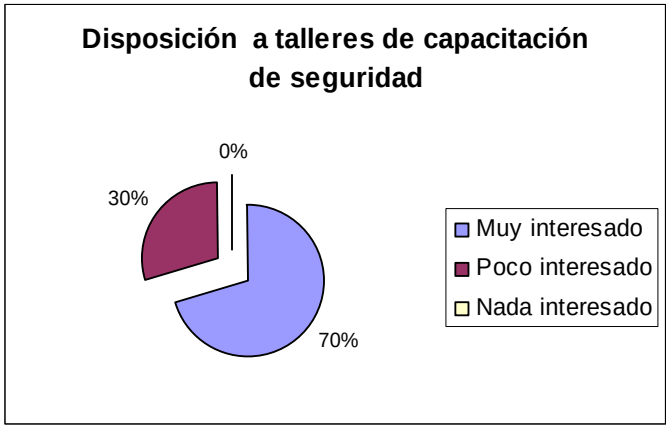
Como se puede apreciar 80% el personal de TIC nunca ha asistido a un evento o taller de seguridad de la información y donde la responsabilidad es compartida entre el área de TIC y las autoridades por considerar a la seguridad de la información no alineada con las decisiones estratégicas de la institución. Sin embargo existe un 20% que ha asistido aproximadamente hace 1 año.

Cuadro Nº 23

¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

Disposición a Talleres de Capacitación	Frecuencia	%
Muy interesado	7	70
Poco interesado	3	30
Nada interesado	0	0
Total	**100**	**100**

Gráfico Nº 23



Análisis Interpretativo

Del personal encuestado un 70% está muy interesado si se realizan programas y talleres de capacitación de seguridad de la información, sin embargo hay un 30% que está poco interesado y con el optimismo de que la situación en la Universidad mejore y se lleve a cabo un plan de gestión de seguridad de la información.

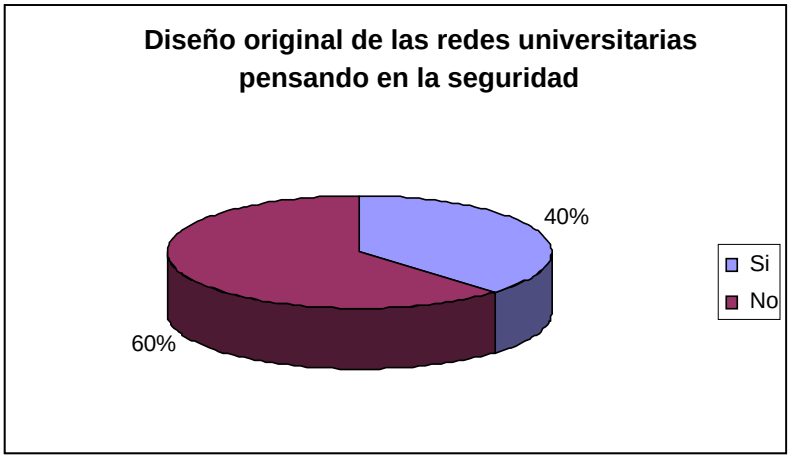
Cuadro Nº 24

¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad . Porqué?

	Frecuencia	%
Si	6	60
No	4	40
Total	10	100

	Razones
Si	• No había Internet y por ende no había riesgos a la información • La Universidad como centro de investigación no debe tener restricciones en el acceso a la información
No	• Se diseñó pensando en la seguridad de acuerdo a la tecnología de ese tiempo

Gráfico Nº 24



Análisis Interpretativo

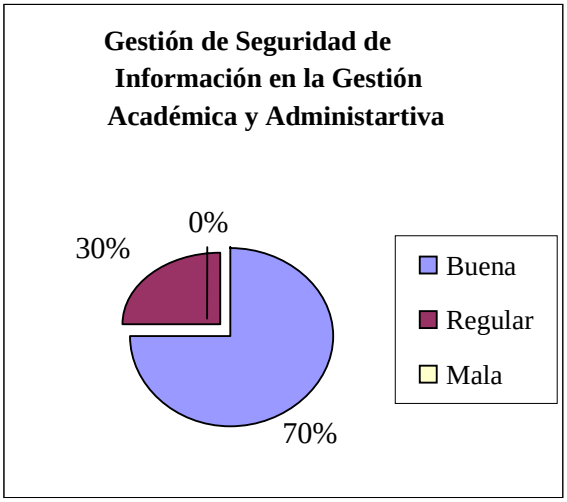
Sobre si las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad un 60% considera que sí, y las razones se han consolidado en el cuadro anterior. Por otra parte un 40% opina lo contrario.

Cuadro Nº 25

¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son: matrícula de alumnos, admisión y registros, tesorería, y trámites documentarios?

	Frecuencia	%
Buena	7	70
Regular	3	30
Mala	0	0
Total	**10**	**100**

Gráfico Nº 25



Análisis Interpretativo

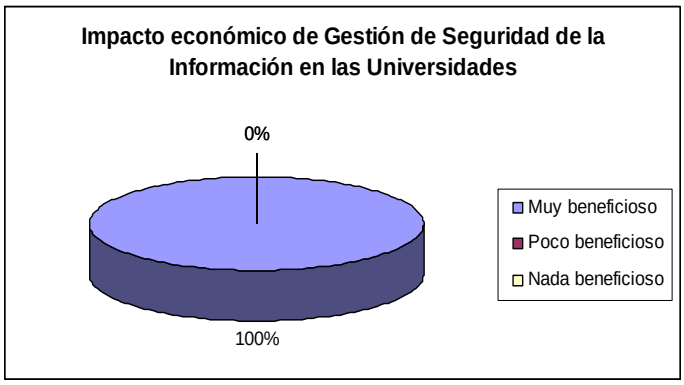
Del total del personal de TIC un 70% considera que la gestión de seguridad de la información en la gestión académica y administrativa es buena, el 30% opina que la gestión es regular pues han sido partícipes de diferentes problemas de seguridad y nadie considera que la gestión de la seguridad es mala.

Cuadro Nº 26

¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?

Impacto económico	Frecuencia	%
Muy beneficioso	10	100
Poco beneficioso	0	0
Nada beneficioso	0	0
Total	**10**	**100**

Gráfico Nº 26



Análisis Interpretativo

Todo el personal encuestado de TIC está de acuerdo que el impacto económico de implementar un plan de gestión de seguridad de la información en la gestión integral de la Universidad va resultar muy beneficioso económicamente.

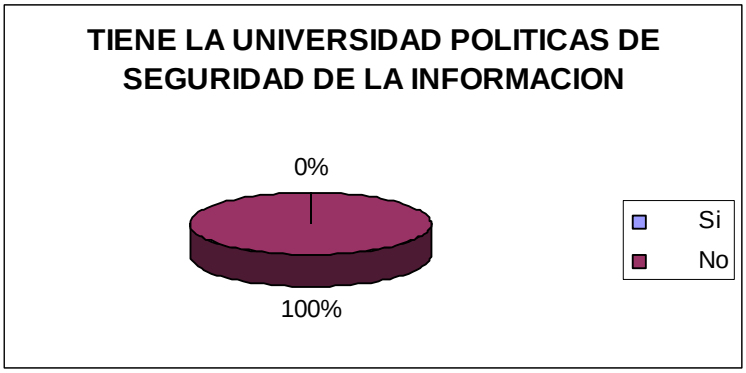
3.1.3 Universidad Privada San Juan Bautista

Cuadro Nº 27

¿En la Universidad donde labora tienen políticas de seguridad de la información?

Opción	Frecuencia
Si	0
No	10

Gráfico Nº 27



Análisis Interpretativo

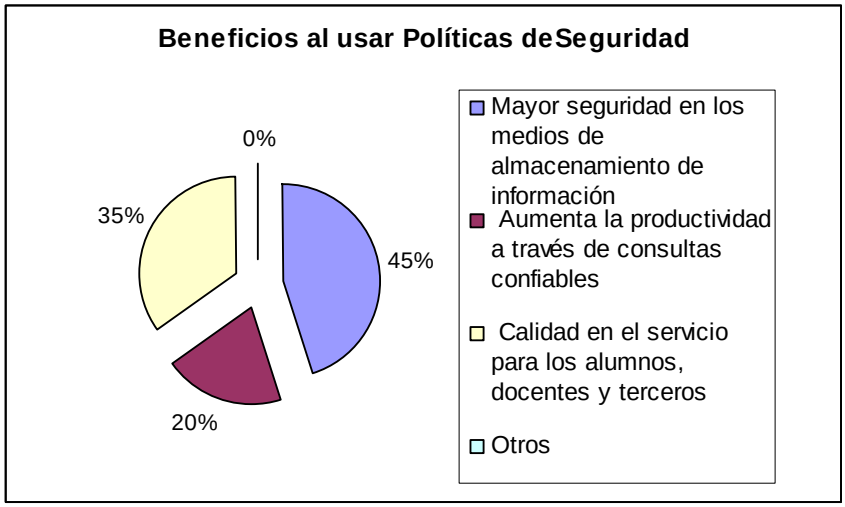
El 100% de los encuestados coincidieron que la Universidad no cuenta con políticas de seguridad de la información.

Cuadro Nº 28

¿Elija que beneficios se presentan cuando la Universidad cuenta con Políticas de Seguridad la información?. Marcar una o más opciones.

Opciones	Frecuencia	%
Mayor seguridad a los medios de almacenamiento de información	9	45
Aumenta la productividad a través de consultas confiables	4	20
Calidad en el servicio para los alumnos, docentes y terceros	7	35
Otros	0	0
Total	**20**	**100**

Gráfico Nº 28



Análisis Interpretativo

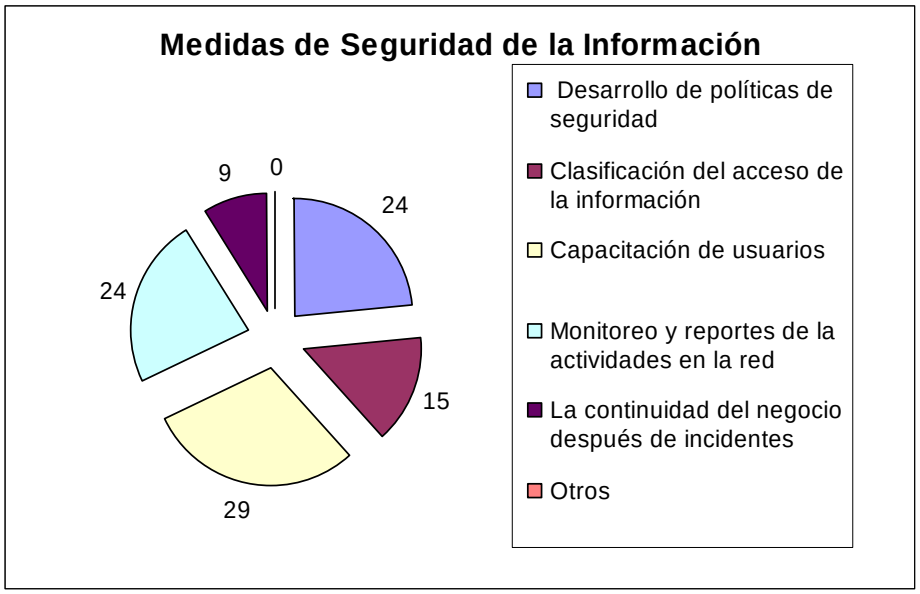
Del total de respuestas marcadas el 45% considera que la mayor seguridad a los medios de almacenamiento de información es uno de los beneficios de usar políticas de seguridad de la información, un 35% apuesta por la calidad en el servicio a los alumnos y docentes, un 20% considera que aumenta la productividad a través de consultas confiables y un 0% no encuentra otro beneficio de los ya mencionados.

Cuadro Nº 29

¿Cuáles de estas medidas de seguridad de la información son las más prioritarias para Usted ? Marcar una o más opciones.

Medidas de Seguridad de la Información	Frecuencia	%
Desarrollo de políticas de seguridad	8	24
Clasificación del acceso de la información	5	15
Capacitación de usuarios	10	29
Monitoreo y reportes de la actividades en la red	8	24
La continuidad del negocio después de incidentes	3	9
Otros	0	0
Total	**34**	**100**

Gráfico Nº 29



Análisis Interpretativo

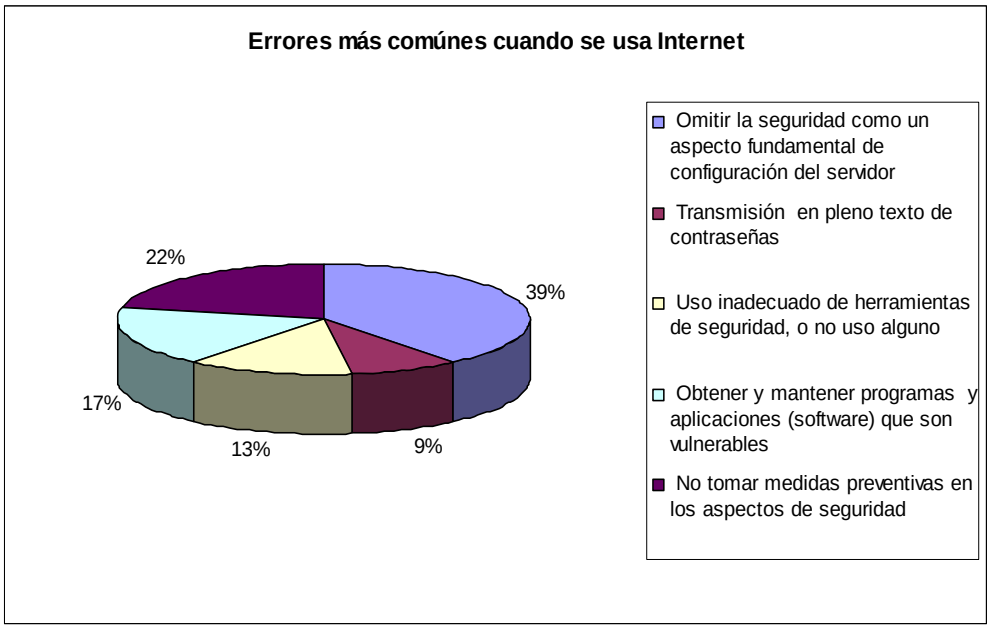
Del total de respuestas obtenidas sobre qué medidas de seguridad consideran más prioritarias un 29% considera la capacitación de los usuarios, un segundo lugar se encuentra el desarrollo de normativas internas y Monitoreo y reportes de las actividades en la red con un 24% y en tercer lugar se encuentran: la clasificación de acceso a la información y la continuidad del negocio después de un incidente con un 15% y 9% respectivamente.

Cuadro Nº 30

¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico? Marcar una o más opciones.

Errores más comunes cuando se usa el correo electrónico y el Internet	Frecuencia	%
Omitir la seguridad como un aspecto fundamental de configuración del Servidor	9	39
Transmisión en pleno texto de contraseñas	2	9
Uso inadecuado de herramientas de seguridad, o no uso alguno	3	13
Obtener y mantener programas y aplicaciones (software) que son vulnerables	4	17
No tomar medidas preventivas en los aspectos de seguridad relevantes	5	22
Total	23	100

Gráfico Nº 30



Análisis Interpretativo

Podemos apreciar que todos los errores mencionados son muy comunes cuando se usa Internet, pero sobresale con más porcentaje "el omitir la seguridad al momento de configurar el servidor " porque es un riesgo muy alto y el servidor puede ser vulnerable al ataque de intrusos.

En la opción otros, personal de TIC coincidieron en un 9% que "no tomar medidas preventivas en los aspectos de seguridad" es un error muy común al usar Internet.

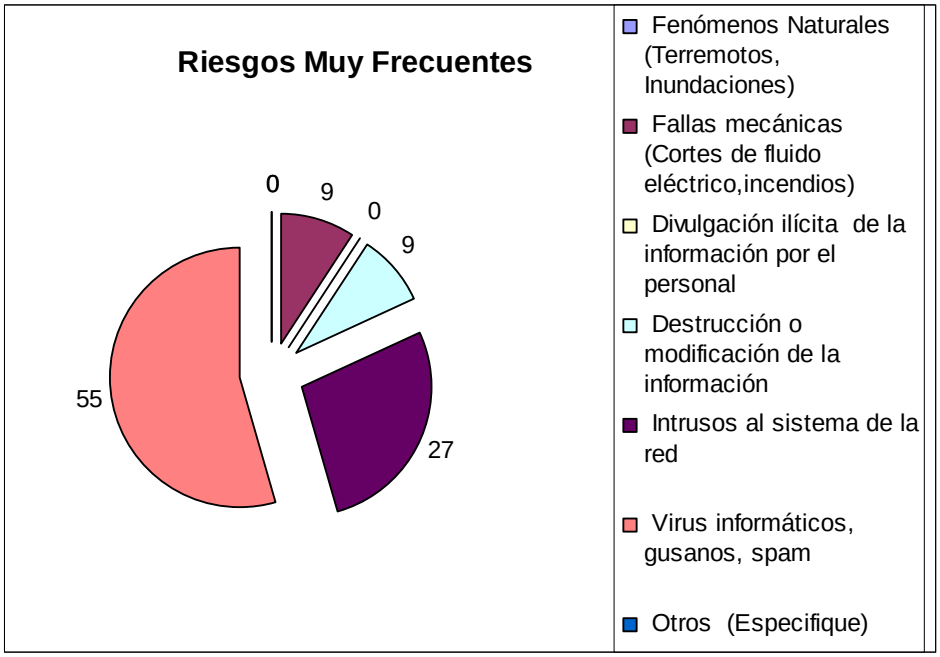
Cuadro Nº 31

¿Cuáles son los riesgos y la frecuencia que se presentan en lo recursos de información?

MF = Muy Frecuente RF = Regularmente frecuente PF = Poco frecuente

Riesgos	MF	%	RF	%	PF	%
Fenómenos Naturales (Terremotos, Inundaciones)	0	0		0	9	41
Fallas mecánicas (Cortes de fluido eléctrico, incendios)	1	9	7	24	2	9
Divulgación ilícita de la información por el personal		0	7	24	3	14
Destrucción o modificación de la información	1	9	4	14	5	23
Intrusos al sistema de la red	3	27	6	21	1	5
Virus informáticos, gusanos, spam	6	55	4	14		0
Otros (Especifique)		0	1	3	2	9
Total	**11**	**100**	**29**	**100**	**22**	**100**

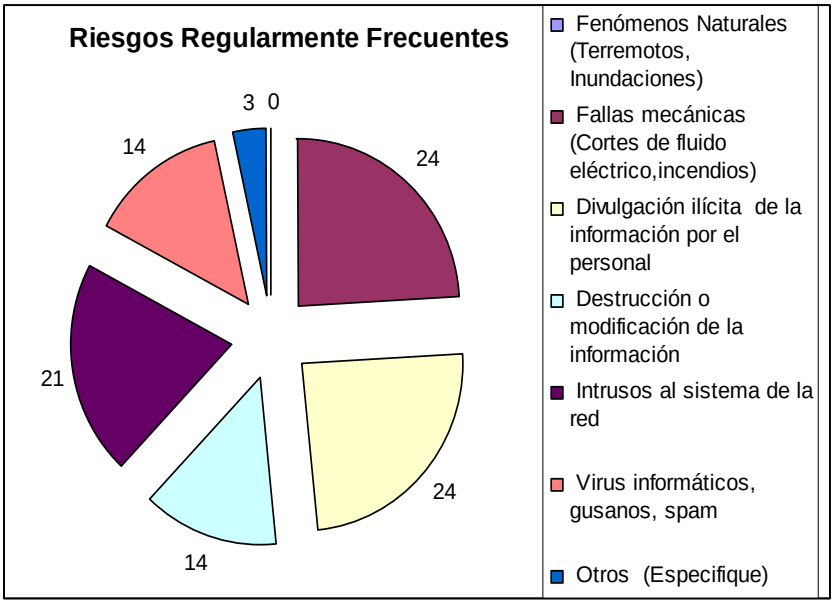
Gráfico Nº 31.1



Análisis Interpretativo

Según el gráfico, los riesgos más frecuentes que se presentan en la Universidad Privada San Juan Bautista son: los virus informáticos, gusanos y spam con un 55%, en segundo lugar están los intrusos al sistema de la red con un 27% y en tercer lugar se encuentran las fallas mecánicas y la destrucción y/o modificación de la información con un 9%.

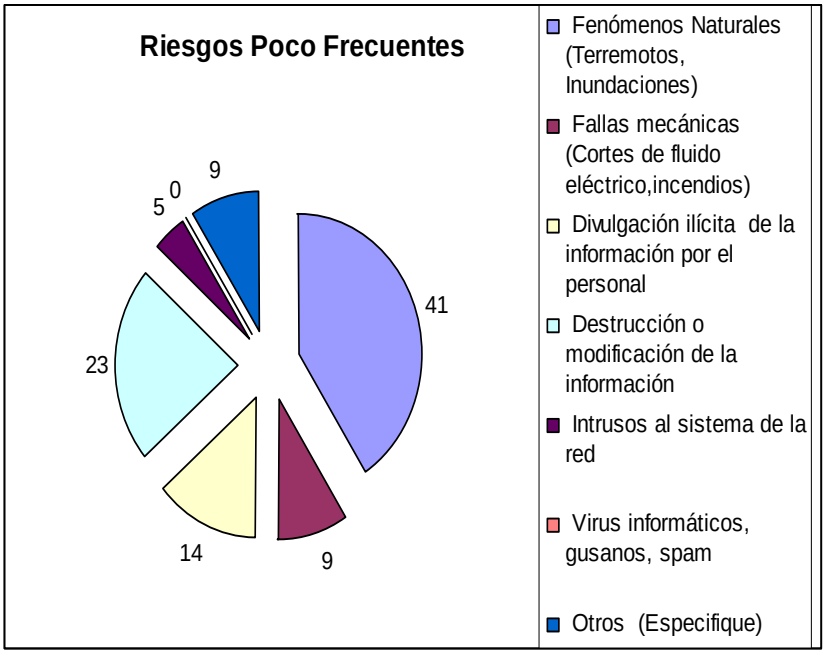
Gráfico Nº 31.2



Análisis Interpretativo

Los riesgos regularmente frecuentes se presentan en su mayoría por las fallas mecánicas (24%) y por la divulgación ilícita de la información por el personal (24%) y en su minoría por fenómenos naturales como terremotos o inundaciones (3%).

Gráfico Nº 31.3



Análisis Interpretativo

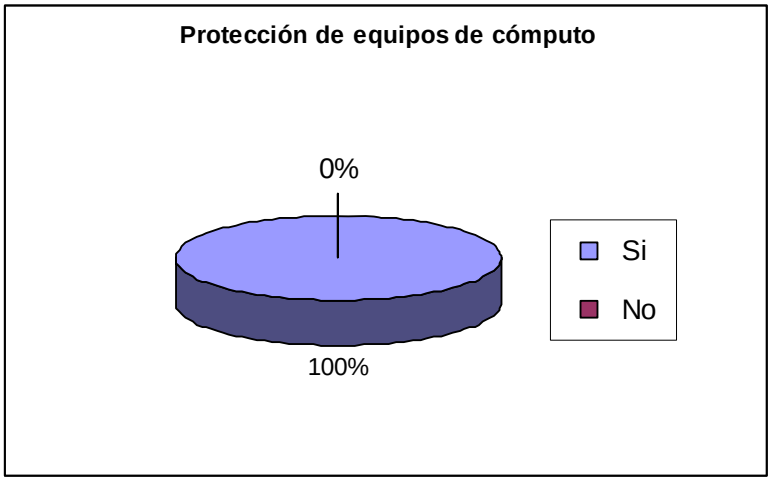
Los riesgos poco frecuentes en su mayoría se presentan por fenómenos naturales (41%) como se puede apreciar en el gráfico y en su minoría se presenta por Intrusos al sistema de la red (5%) debido a que la Universidad ha implementado mecanismos de seguridad ante amenazas externas a la información.

Cuadro Nº 32

¿Sus equipos de cómputo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de energía eléctrica?

Protección de equipos cómputo	Frecuencia	%
Si	10	100
No	0	0
Total	**10**	**100**

Gráfico Nº 32



Análisis Interpretativo

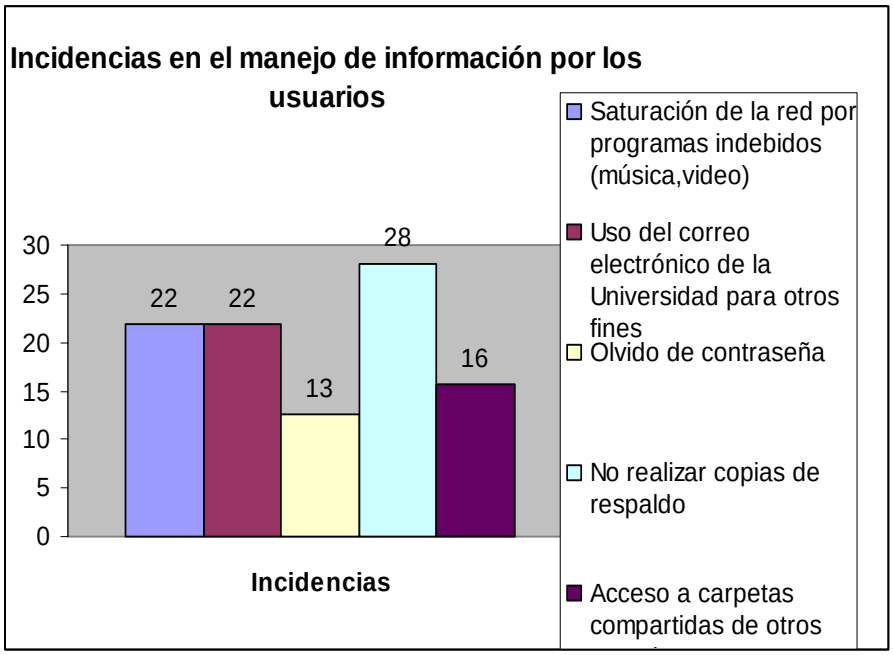
Los equipos de cómputo en las oficinas están protegidos al 100% ante cortes de energía eléctrica por UPS y generadores de energía eléctrica.

Cuadro Nº 33

¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

Incidencias que se dan con más frecuencia	Frecuencia	%
Saturación de la red por programas indebidos (música, video)	7	22
Uso del correo electrónico de la Universidad para otros fines	7	22
Olvido de contraseña	4	13
No realizar copias de respaldo	9	28
Otros : Acceso a carpetas compartidas de otros usuarios	5	16
Total	32	100

Gráfico Nº 33



Análisis Interpretativo

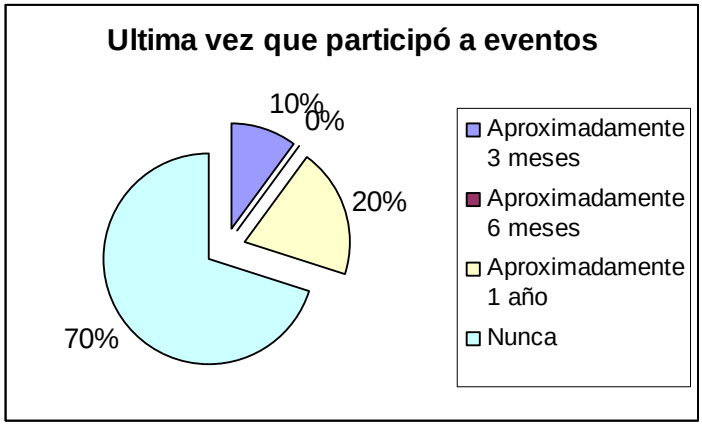
Del total de respuestas recogidas el 28% considera que una de las incidencias por parte de los usuarios es que no hacen copias de respaldo cuando realizan sus trabajos, en un 22% se encuentran: la saturación de la red e Internet por programas indebidos y el uso del correo de la Universidad para fines personales, lo cual deja mucho que desear con la ética profesional de la persona que maneja información. En la opción otros, un 16% de respuestas coincidieron que existen usuarios que dedican su tiempo a explorar y acceder a carpetas compartidas ajenas. Por último también es preocupante el olvido de contraseñas (13%).

Cuadro Nº 34

¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

Ultima vez que participó a eventos de seguridad de la información	Frecuencia	%
Aproximadamente 3 meses	1	10
Aproximadamente 6 meses	0	0
Aproximadamente 1 año	2	20
Nunca	7	70
Total	10	100

Gráfico Nº 34



Análisis Interpretativo

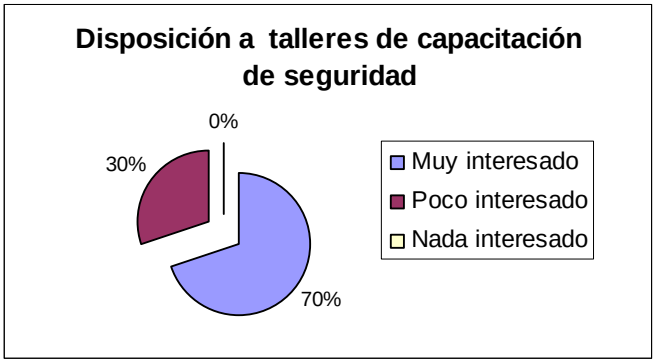
Como se puede apreciar el 70% del personal de TIC de la Universidad nunca ha asistido a eventos o talleres de seguridad de la información, un 20% ha asistido aproximadamente hace 1 año y dentro de la opción otros, un 10% ha participado aproximadamente hace 3 meses.

Cuadro Nº 35

¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

Disposición de asistir a talleres de capacitación	Frecuencia	%
Muy interesado	7	70
Poco interesado	3	30
Nada interesado	0	0
Total	**10**	**100**

Gráfico Nº 35



Análisis Interpretativo

El personal encuestado se siente muy interesado (70%) si se realizan programas y talleres de capacitación de seguridad, esto es muy importante porque permitirá que se encuentren identificados y comprometidos con la información confidencial que manejan. Hay que resaltar también que un 30% se siente poco interesado y no hay ningún encuestado que sea indiferente a estos eventos de capacitación de seguridad.

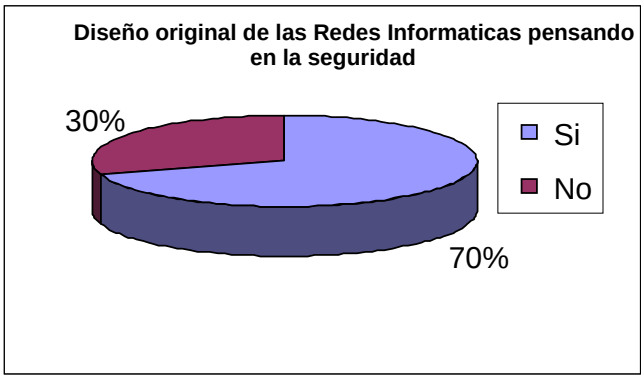
Cuadro Nº 36

¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad. Porqué?

	Frecuencia	%
Si	7	70
No	3	30
Total	10	100

	Razones
Si	• No había Internet y por ende no había riesgos a la información • La Universidad como centro de investigación no debe tener restricciones en el acceso a la información • No se previó el creciente avance tecnológico y de las comunicaciones
No	• Se diseñó pensando en la seguridad de acuerdo a la tecnología de ese tiempo

Gráfico Nº 36



Análisis Interpretativo

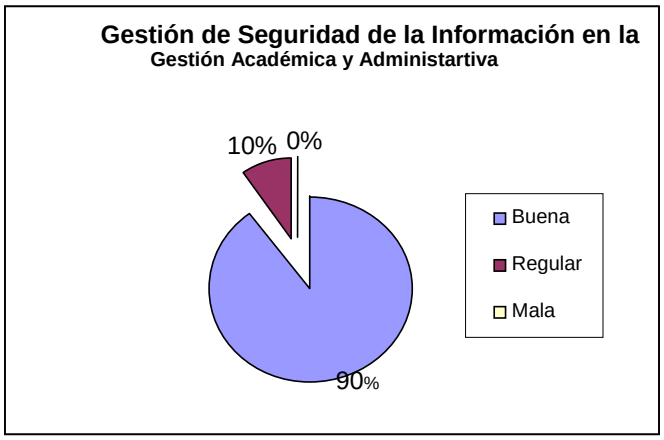
Sobre si las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad un 70% considera que sí, y las razones se han consolidado en el cuadro anterior. Por otra parte un 30% opina lo contrario.

Cuadro Nº 37

¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son: matrícula de alumnos, admisión y registros, tesorería, y trámites documentarios?

	Frecuencia	%
Buena	9	90
Regular	1	10
Mala	0	0
Total	**10**	**100**

Gráfico Nº 37



Análisis Interpretativo

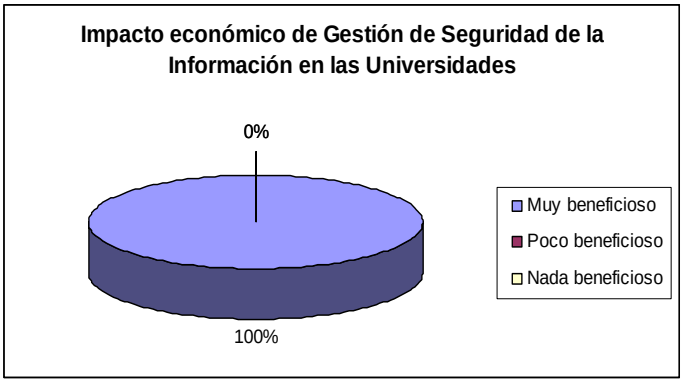
La mayoría (90 %) considera que la gestión de seguridad de la información en la gestión académica y administrativa es buena y solamente un 10% del personal encuestado opina que la gestión de la seguridad es regular.

Cuadro Nº 38

¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?

Impacto económico	Frecuencia	%
Muy beneficioso	10	100
Poco beneficioso	0	0
Nada beneficioso	0	0
Total	**10**	**100**

Gráfico Nº 38



Análisis Interpretativo

Todo el personal encuestado de TIC está de acuerdo que el implementar un plan de gestión de seguridad de la información en la gestión integral de la Universidad va resultar muy beneficioso económicamente, y nadie opina lo contrario.

3.4 PRUEBA DE HIPOTESIS

Hipótesis Auxiliar Nº 1

Las Universidades que implementen políticas de seguridad de la información minimizan los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios.

En el cuadro Nº 39 se ha consolidado los resultados de la encuesta de las 3 universidades para validar la hipótesis.

Cuadro Nº 39

Universidades	Estrategia de Gestión de seguridad de la información	Riesgos muy frecuentes		
	Desarrollo de políticas de seguridad (%)	Divulgación Ilícita de Información (%)	Intrusos en la red (%)	Virus infor-máticos (%)
UPSJB	24	0	27	55
UNFV	19	36	18	36
UNMSM	37	0	22	56

Fuente: *Elaboración propia*

Análisis

En la UPSJB del total de encuestas sobre qué estrategias de seguridad son las más prioritarias, se consideró la implementación de políticas de seguridad (24%) para reducir los riesgos muy frecuentes que se presentan en la Universidad como son los intrusos tanto internos como externos que ocasionan graves problemas en la red (27%) y el otro riesgo muy frecuente son los virus informáticos (55%).

En la UNFV el desarrollo de políticas de seguridad de la información (19%) va permitir que se reduzcan los riesgos como la divulgación ilícita de la información que sucede con mucha frecuencia con el personal (36%) y la presencia de los virus informáticos (36%), esto debido a que el usuario que maneja la información no toma conciencia de lo vital que es su trabajo.

En la UNMSM el desarrollo de políticas de seguridad (37%) y el cumplimiento de las normativas y procedimientos va reducir el número de programa infectados con virus informáticos pues alcanza un 56%.

Este análisis nos permite comprobar que las Universidades que implementen políticas de seguridad de la información minimizarán los riesgos de la información como son la divulgación ilícita de la información por parte de los trabajadores y la presencia de los virus informáticos que son muy frecuentes en las universidades encuestadas.

Por otra parte, los resultados que se obtuvo de la Primera Encuesta Nacional de Seguridad de la Información-2004 de la Presidencia del Consejo de Ministros – ONGEI también han servido para validar esta hipótesis.
Sobre los tipos de incidentes o riesgos más frecuentes que ha tenido las instituciones se obtuvieron los siguientes resultados:

- El 86% de las instituciones ha tenido incidentes de virus informático.
- El 19% de las instituciones ha tenido incidentes de Acceso no autorizado por personal interno
- EL 10% de las instituciones ha tenido incidentes de Robo de información confidencial.

Hipótesis Auxiliar Nº 2

La gestión de seguridad de la información contribuye a la calidad en el servicio y en la protección de los sistemas de información como son matrícula de alumnos, admisión y registros, cobranzas, y trámites documentarios en las Universidades

En el cuadro Nº 40 se ha consolidado los resultados de la encuesta de las 3 universidades para validar la hipótesis.

Cuadro Nº 40

Universidades	Beneficios de la gestión de la seguridad de la información			Impacto en la gestión académica y administrativa		
	Mejor protección de la información (%)	Calidad en el servicio a los alumnos, docentes	Aumenta la productividad a través de consultas directas y confiables (%)	Muy buena (%)	Regular (%)	Mala (%)
UPSJB	45	35	20	90	10	0
UNFV	50	21	29	75	25	0
UNMSM	50	25	25	90	10	0

Fuente: *Elaboración propia*

Análisis

En la UPSJB consideran que los principales beneficios que genera la gestión de seguridad de la información es la mejor protección de la información (45%) y la calidad en el servicio a los alumnos, docentes y terceros (35%) esto genera un impacto positivo en la gestión administrativa y académica con los sistemas de información (90%) como son matrícula de alumnos, tesorería, trámites documentarios, etc

En la UNFV también consideran como beneficio importante de la gestión de seguridad, la mejor protección de la información (50%) y también aumenta la productividad a través de consultas confiables (29%) y luego la calidad en el servicio a los alumnos (21%) estas apreciaciones ha generado un impacto aceptable en la gestión administrativa y académica con un 75 % como buena y un 25% como regular.

En la UNMSM al igual que las otras universidades, la mejor protección de la información es uno de los beneficios más importantes (50%) seguido de la calidad en el servicio a los alumnos (25%) esto da como consecuencia al igual que la UPSJB un impacto positivo a la gestión administrativa y académica con los sistemas de información.

Este análisis nos permite comprobar que con la gestión de seguridad de la información se obtienen beneficios como una mejor protección de los recursos de información (sistemas de información, redes, etc), una mejor calidad en el servicio a los alumnos y docentes y

va tener un impacto muy positivo cuando hagan uso de los servicios universitarios reflejados en los sistemas de información que brindan las Universidades.

Comprobamos esta hipótesis con la encuesta nacional de la ONGEI donde se obtuvieron los siguientes resultados:

- En el 78% de las instituciones los sistemas informáticos críticos si están aislados de personal no autorizado.
- El 54% de las instituciones si tienen mecanismos de monitoreo del uso de los Sistemas informáticos.
- El 65% de las instituciones si tienen políticas y mecanismos de protección de datos y privacidad de la información del personal de la institución.

Hipótesis Auxiliar Nº 3

Los programas y talleres de capacitación de seguridad de la información crean conciencia de seguridad en los trabajadores, docentes, alumnos y terceros para un buen uso de la información.

En el cuadro Nº 41 se ha consolidado los resultados de la encuesta de las 3 universidades para validar la hipótesis.

Cuadro Nº 41

Universidades	Incidencias de seguridad de los usuarios			Asistencia a talleres de capacitación	Interés en capacitación de seguridad
	Saturación de la red (%)	No hacer copias de seguridad (%)	Divulgación de la Informa-ción (%)	Nunca (%)	Muy interesado (%)
UPSJB	22	28	16	70	70
UNFV	35	17	13	100	70
UNMSM	29	18	6	20	80

Fuente: *Elaboración propia*

Análisis

Podemos apreciar en el cuadro, que las incidencias de seguridad por parte de los usuarios de las Universidades investigadas son parecidas, en la UPSJB resalta con más incidencia el no hacer copias de seguridad por parte de los usuarios (28%), en la UNFV y UNMSM resalta la saturación de la red por programa indebidos con un 35% y 29% respectivamente. En cuanto a la asistencia de eventos seguridad de la información para la capacitación, están muy interesados tanto de la UPSJB y UNFV con un 70% y en la UNMSM demuestran un interés el 80%.

Este análisis nos permite comprobar que los programas de capacitación, talleres, eventos y lecturas con respecto a la seguridad de la información va crear conciencia en los trabajadores, alumnos y docentes para que se sientan identificados con la información que manejan y se reduzca el número de incidencias de seguridad como saturación de la red por programas indebidos (música, video, etc.), divulgación de la información, etc.

Comprobamos esta hipótesis con la encuesta nacional de la ONGEI donde se obtuvieron los siguientes resultados:

- En el 80% de las instituciones, los usuarios no reciben capacitación en temas de seguridad de la información
- El 85% de las instituciones no tienen asesoramiento especializado en materia de seguridad de la información
- En el 68% de las Instituciones, los usuarios no están preparados para reportar los incidentes de la seguridad de los Sistemas de información.

Hipótesis Auxiliar Nº 4

El rediseño la red informática universitaria permite un tráfico de la información más seguro y un servicio eficaz a los trabajadores, alumnos, docentes y terceros.

En el cuadro Nº 42 se ha consolidado los resultados de la encuesta de las 3 universidades para validar la hipótesis.

Cuadro Nº 42

Universidades	Se diseñó la red informática sin pensar en la seguridad (%)
UPSJB	70
UNFV	60
UNMSM	70

Fuente : *Elaboración propia*

Análisis

Los expertos consultados de las 3 universidades estuvieron de acuerdo que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad. Las razones fueron las siguientes: Antes no había Internet por tanto no había riesgos, no se previó el crecimiento exponencial de la tecnología y comunicaciones y todavía existe la idea de que la Universidad como centro de investigación no debe tener restricciones. El rediseño de las redes informáticas universitarias permite segmentar el área académica con la administrativa de tal forma que por ejemplo los alumnos con conocimientos de tecnología no puedan accesar a información confidencial de la institución. Asimismo, va permitir un tráfico más seguro y una mejor calidad en el servicio a los alumnos, docentes, trabajadores y terceros.

Comprobamos esta hipótesis con la encuesta nacional de la ONGEI donde se obtuvieron los siguientes resultados:

- El 82% de las instituciones planea usar Firewalls
- El 71% de las instituciones planea usar Sistemas de detección de intrusos
- El 58% de las instituciones planea usar Redes Privadas Virtuales

CAPITULO IV
PROPUESTA DE UN PLAN DE SEGURIDAD DE LA INFORMACION PARA LAS UNIVERSIDADES

4.1 SITUACION ACTUAL

Efectuado el diagnóstico de las tres Universidades de Lima Metropolitana, hemos observado que las Universidades carecen en general de una metodología, guía o marco de trabajo que ayude a la identificación de riesgos y vulnerabilidades. A continuación mencionamos los siguientes aspectos críticos:

- ***Políticas de seguridad***. Dentro de los diferentes aspectos a considerar en la gestión de seguridad de la información que brindan las universidades se ha podido observar que en su mayoría no tienen políticas de seguridad de la información, y si las tienen no las cumplen en la práctica. Muchas veces no cumplen con las políticas de seguridad porque simplemente desconocen de estas buenas prácticas de seguridad y no toman conciencia del rol que cumplen cuando manejan información confidencial. El cuadro Nº 43 corrobora lo mencionado:

Cuadro Nº 43

Universidades	Tienen políticas		Se cumplen las políticas de Seguridad de la Información		
	Si (%)	No (%)	A cabalidad (%)	Medianamente (%)	No se cumple (%)
UPSJB	0	100	0	0	0
UNFV	60	40	40	60	0
UNMSM	90	10	33	67	0

Fuente: *Elaboración propia*

- ***Protección de los equipos de cómputo***. No todas las universidades están preparadas para mantener el correcto funcionamiento del suministro eléctrico pues en sus áreas académicas y administrativas no cuentan con un sistema de alimentación ininterrumpida de energía (UPS) o generadores de energía según el cuadro Nº 44. Es importante un sistema de UPS para apoyar un cierre ordenado o el funcionamiento de los equipos que soporten operaciones críticas dentro de las actividades de la Universidad.

Cuadro Nº 44

Universidades	Protección a los equipos de cómputo	
	Si (%)	No (%)
UPSJB	100	0
UNFV	30	70
UNMSM	60	40

Fuente: *Elaboración propia*

- ***Capacitación***. La mayoría del personal de TIC de las Universidades no están capacitados en temas actuales de seguridad de la información y lo más preocupante es que nunca han asistido a eventos o talleres de seguridad como se puede apreciar en el cuadro Nº 45. En muchas instituciones no existe una cultura de seguridad debidamente arraigada en todos los niveles incluyendo los directivos, quiénes no toman conciencia que la capacitación en seguridad de la información debe estar alineada con las estrategias de la institución.

Cuadro Nº 45

Universidades	Asistencia a eventos de seguridad de la información		
	Hace 6 Meses (%)	Hace 1 año (%)	Nunca (%)
UPSJB	0	30	70
UNFV	0	0	100
UNMSM	40	40	20

Fuente: *Elaboración propia*

- ***Incidencias de seguridad***. El cuadro Nº 46 nos muestra las incidencias de seguridad por los usuarios que manejan la información, y que ocurren muchas veces por descuido, desconocimientos técnicos o porque simplemente no cumplen con las normas internas de seguridad de las instituciones. Los incidentes de seguridad más devastadores tienden a ser más internos que externos. La gestión de la seguridad de la información necesita como mínimo la participación de todos los empleados de la Universidad, además de la participación de los docentes, alumnos y proveedores.

Cuadro Nº 46

Universidades	Incidencias de seguridad que ocasionan los usuarios			
	Olvido de Contraseñas (%)	Saturación de la red por programas prohibidos (%)	No hacer copias de seguridad (%)	Divulgación de la Información (%)
UPSJB	13	22	28	16
UNFV	13	35	17	13
UNMSM	12	29	18	6

Fuente: *Elaboración propia*

- ***Riesgos más frecuentes***. También hemos observado que las Universidades carecen en general de una metodología, que ayude a la identificación de riesgos y vulnerabilidades y cuenten con mecanismos de control para mitigar los mismos. El cuadro Nº 47 presenta los riesgos más frecuentes que se presentan en las universidades:

Cuadro Nº 47

Universidades	Riesgos más frecuentes				
	Cortes de energía eléctrica (%)	Destrucción o modificación de la información (%)	Divulgación Ilícita de Información (%)	Intrusos en la red (%)	Virus infor-máticos (%)
UPSJB	9	9	0	27	55
UNFV	0	9	36	18	36
UNMSM	11	11	0	22	56

Fuente: *Elaboración propia*

- ***Redes informáticas universitarias***. Las universidades corren mayor riesgo que la mayoría de las grandes corporaciones porque utilizan redes informáticas abiertas, comunicativas y descentralizadas, generalmente con diversos niveles de seguridad. La consulta a expertos de TIC de las 3 Universidades encuestadas sobre: ¿Las redes informáticas universitarias fueron diseñadas pensando originalmente en la seguridad? ¿Por qué?. Las razones se describen en el cuadro Nº 48.

Cuadro Nº 48

	Razones
Si	• No había Internet y por tanto no había riesgos de seguridad de la información • No se previó el vasto y rápido desarrollo tecnológico y de comunicaciones • La Universidad como centro de investigación no debe tener restricciones de acceso a los recursos de la información
No	• Se diseñó pensando en la seguridad de acuerdo a la tecnología de ese tiempo

Fuente: *Elaboración propia*

4.2 OBJETIVOS

- Lograr el compromiso de la Dirección con la Seguridad de la Información
- Asignar roles y responsabilidades a personal de la Institución para la Seguridad de la Información
- Determinar los requerimientos de seguridad y evaluar los riesgos y la administración de los mismos.
- Establecer la necesidad de educar e informar a toda la comunidad universitaria sobre materias de seguridad de la información.
- Controlar y prevenir los accesos no autorizados de la información
- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

4.3 EVALUACION DE RIESGOS Y VULNERABILIDADES Y ESTRATEGIAS DE SEGURIDAD

En este cuadro se muestran los riesgos y vulnerabilidades identificadas y las estrategias o medidas de seguridad necesarias para mitigar dichos riesgos.

Riesgos / Vulnerabilidades	Estrategias o medidas de seguridad a Aplicar
• Interés en obtener información estratégica de la Universidad por parte de la competencia, tales como información de postulantes para examen de admisión, información de alumnos regulares, planilla de pagos de docentes, etc. • Personal que trabaja la Universidad que se puede prestar para estas actividades desleales.	• Estándares de seguridad para servidores con sistemas operativos Windows y Linux. • Restricciones en el manejo de la información enviada por correo electrónico hacia redes externas. • Revisiones periódicas de los registros de los sistemas y operaciones realizadas por los usuarios

Pérdida de información ocasionada por la infección de virus informático.	• Adecuada arquitectura e implementación del sistema antivirus • Verificación periódica de la actualización del antivirus de computadoras personales y servidores. • Generación periódica de reporte de virus detectados.
Ausencia o exceso de contraseñas manejadas por los usuarios	• Uniformizar dentro de lo posible la estructura de las contraseñas empleadas y sus fechas de renovación • Implementar un sistema de Servicio de Directorio, el cual permita al usuario identificarse en él, y mediante un proceso automático, éste lo identifique en los sistemas en los cuales posee acceso.
Falta de conciencia en seguridad de la información por parte del personal de la Universidad.	• Programa de capacitación de la Universidad en temas relacionados a la seguridad de la información.
Arquitectura de red inapropiada para controlar accesos desde redes externas. Posibilidad de acceso no autorizado a sistemas por parte de personal externo a la Universidad.	• Diseño de arquitectura de seguridad de red. • Adecuada configuración de elementos de control de conexiones (Firewalls) • Implementación y administración de herramientas de seguridad
No existen controles con respecto a las copias de seguridad. Se realizan copias de seguridad pero muchas veces no se ha probado que se puede recuperar la	• Establecimiento de un procedimiento formal que contemple la generación de una copia de respaldo para los

información.	usuarios. • Asegurar que la información del usuario se almacene en el servidor y estén protegidas por una contraseña. • Enviar fuera de la oficina una copia de seguridad completa una vez por semana.
No existe un control de protección sobre los correos electrónicos no solicitados por los usuarios	• Implementación y administración de herramientas para la inspección del contenido de los correos electrónicos recibidos
Acceso abierto a redes inalámbricas por parte de intrusos	• Separación del segmento de red Inalámbrico mediante un firewall. • Configuración la red inalámbrica para permitir el tráfico sólo de los equipos de escritorio y portátiles de la oficina.

4.4 POLITICAS DE SEGURIDAD DE LA INFORMACION

Se elaborarán las políticas de seguridad con el propósito de proteger la información de la Universidad, éstas servirán de guía para la implementación de un plan de seguridad que contribuirá a mejorar la disponibilidad, la integridad y la confiabilidad de la información dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales de la Universidad.

Alcance

Estas políticas están dirigidas a los empleados docentes, empleados administrativos, estudiantes, contratistas, consultores y demás miembros de la comunidad universitaria, incluyendo el personal externo que presta servicios a la universidad y que usa tecnología de información. Estas políticas aplican a los equipos propios o arrendados que tiene la universidad y a los equipos propiedad de personas

que sean conectados a las redes de la universidad. La garantía del cumplimiento de estas políticas será responsabilidad de cada miembro de la comunidad universitaria pues su contravención afecta a toda la universidad.

A continuación definimos las siguientes políticas de seguridad de la información :

4.4.1 Organización de la seguridad

Se tiene como objetivo gestionar la seguridad dentro de la institución. Sugiere diseñar una estructura de administración que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

En esta política se definen los roles y responsabilidades a lo largo de la Universidad con respecto a la protección de los recursos de información. Los miembros de la comunidad universitaria deben tener el criterio para decidir cuando pueden hacer uso personal de los recursos de información y serán responsables de dicha decisión. De igual manera, el área de seguridad de la información es responsable de crear unas normas internas de uso personal de los servicios de Internet y de la red de la Universidad. Los empleados, docentes o estudiantes deben guiarse por las políticas de la Universidad sobre uso personal, y si hay incertidumbre, los deben consultar de inmediato con los directivos de la institución.

4.4.2 Inventario de activos

Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos de información. El proceso de constituir un inventario de activos es un aspecto importante de la gestión de riesgos. La Universidad debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la organización puede entonces, asignar niveles de protección proporcionales al valor e importancia de los activos. Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información. Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación

vigente del mismo. Ejemplos de activos asociados a los recursos de información son los siguientes:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida, información archivada.
- Recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (Routers, Pbs., contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

4.4.3 Clasificación de la información

El objetivo es asegurar un nivel de protección adecuado a los activos de la información. La información debería clasificarse para indicar la necesidad, prioridades y grado de protección. La información y los resultados de los sistemas que manejan datos clasificados deberían catalogarse en relación con su valor e importancia para la organización. También puede ser adecuado catalogar la información en términos de criticidad por ejemplo de su integridad y disponibilidad para la institución.

La clasificación de la información debe ser documentada por el propietario de la información, aprobada por la dirección responsable y distribuida al personal del área de sistemas de información durante el proceso de desarrollo de sistemas o antes de la distribución de los documentos o datos. La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe tener la misma clasificación sin importar el

formato. Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, cuando la información se ha hecho pública.

La información debe ser examinada para determinar el impacto en la Universidad si fuera divulgada o alterada por medios no autorizados. A continuación detallamos algunos ejemplos de información sensible:

- Registros de alumnos
- Cuenta Corriente de alumnos
- Lista de rubros de pagos a la Universidad (tarifas)
- Registros de Grados y títulos de alumnos
- Carga académica de docentes
- Registros del personal administrativo
- Datos financieros de la Universidad

4.4.4 Seguridad del Personal

- *Seguridad en la definición de los puestos de trabajo y recursos.* El departamento de Recursos Humanos debe notificar al área de Seguridad de la Información, la renuncia o despido de los empleados así como el inicio y fin de los períodos de vacaciones de los mismos. Cuando se notifique el despido o transferencia, el personal del área debe de asegurarse que la cuenta de usuario sea revocado. Cualquier ítem entregado al empleado o al proveedor como computadoras portátiles, llaves, software, datos, documentación, manuales, etc. Deben ser entregados a su gerente o al área de Recursos Humanos.
- *Capacitación de Usuarios.* Los empleados de la Universidad deben recibir la formación adecuada y actualizaciones regulares de las políticas y procedimientos de la institución, donde se incluya los requisitos de seguridad, responsabilidades legales, así como prácticas en el uso correcto de los recursos de tratamiento de la información (Procedimientos de conexión, uso de paquetes de software, etc.) antes de obtener acceso a la información o los servicios.
- *Procedimientos de respuestas ante incidentes de seguridad.* Si un empleado de la Universidad detecta o sospecha la ocurrencia de un incidente de

seguridad, tiene la obligación de notificarlo al personal de seguridad de la información o directamente al proveedor de servicio. Bajo ninguna circunstancia los usuarios deben de probar las sospechas de vulnerabilidad o fallas del sistema. El área de seguridad de la información debe documentar todos los reportes de incidentes de seguridad.

4.4.5 Control de Acceso a los datos

a) La interfaz de usuario para acceder a la información disponible en los sistemas debe ser clasificada como confidencial o no. *Ejemplos posibles de* información que se considera confidencial son “los datos de los aspirantes a especialidades de pregrado”, “las historias clínicas de los alumnos”, “información de investigaciones académicas en curso cuyos resultados sean críticos para la competitividad de la universidad y de los grupos de investigación” y “los expedientes de la oficina de Grados y Títulos”. Las personas que estén involucradas con este tipo de información deben seguir procedimientos adecuados para evitar el acceso sin autorización a esta información.

b) Tenga claves seguras y no comparta su cuenta. Los usuarios autorizados son los responsables por la seguridad de su cuenta y de su clave. Las claves de los usuarios con privilegios deben cambiarse mínimo cada mes y las claves de los usuarios sin privilegios deben cambiarse mínimo cada tres meses.

c) En medios electrónicos debe tener controles de acceso individuales (clave personal) y se recomienda que los archivos se almacenen encriptados. La seguridad física es muy importante para este tipo de información, así que el equipo donde sea almacenada debe estar asegurado físicamente y debe conectarse a las redes de la universidad sólo cuando las necesite (idealmente, el equipo donde se almacena la información debe sólo ser utilizado por las personas autorizadas a tener acceso a dicha información). Entre los métodos que se pueden utilizar para garantizar esto está el uso de llaves que aseguran el hardware del equipo para poder ser encendido. Si es un equipo portátil nunca debe dejarlo solo y siempre debe utilizar el cable de aseguramiento (lockdown cable) y cuando salga de la oficina asegúrese que el equipo

y cualquier material crítico queden bajo llave. En caso de que la información sea muy importante no se debe dudar en guardar los medios y los equipos en una caja fuerte.

d) Si después de utilizar este tipo de información no se hará pública y no se necesita para procesos posteriores, destrúyala (una picadora de papel para estos fines puede ser utilizada o puede incinerarla) o depositarla en los tachos de basura de la Universidad rompiendo antes el documento (aquí se supone que las personas encargadas de retirar el contenido de los tachos labora con la universidad y realiza un manejo correcto de los desechos); los datos en medio electrónico deben ser borrados de manera confiable (no basta con emitir el comando de borrado, es aconsejable hacer dos cosas adicionales: desocupar la papelera de reciclaje y reescribir el disco con otro archivo que tenga el mismo nombre del que fue borrado, en el mismo directorio donde estaba ubicado).

e) Todas las conexiones de red internas y externas deben cumplir con las políticas de la Universidad sobre servicios de red y control de acceso. Es responsabilidad del área de sistemas y del área de seguridad de la información determinar: los elementos de red que pueden ser accedidos, el procedimiento de autorización para la obtención de acceso y controles para la protección de la red.

Las siguientes actividades están prohibidas:

- Copia no autorizada de material protegido por derechos de autor que incluye, pero no está limitado a, digitalización y distribución de imágenes o fotografías de cualquier origen (revistas, libros, páginas web, etcétera), digitalización y distribución de música, audio o video, distribución e instalación de software de los cuales ni la universidad ni el usuario tienen la licencia debida.

- Exportar software, información técnica, software y tecnologías para criptografía en contra de leyes de control regionales o internacionales. Las dependencias apropiadas (área de sistemas de información y asesoría legal) deben ser consultadas antes de exportar cualquier material de este tipo.

- Revelar la clave ó código de su cuenta a otros (por ejemplo, su cuenta de correo electrónico, su usuario de bases de datos, su código para realizar llamadas de

larga distancia) o permitir su uso a terceros para actividades ajenas a la misión de la universidad. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario, docente o estudiante cuando la actividad se realiza desde el hogar (por ejemplo, computadores portátiles, teléfonos celulares o agendas electrónicas propiedad de la universidad).

- Utilizar la infraestructura de tecnología de información de la universidad para conseguir o transmitir material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de comunicaciones de la universidad con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.

- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de la universidad.

- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios. Entre las acciones que contravienen la seguridad de la red se encuentran, aunque no están limitadas, acceder a datos cuyo destinatario no es usted, ingresar a una cuenta de un servidor o de una aplicación para la cual no está autorizado.

- Está prohibido explícitamente el monitoreo de puertos o análisis de tráfico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas responsables de la seguridad de la información pueden realizar estas actividades cuando se realicen en coordinación con el personal responsable de los servidores, los servicios, las aplicaciones y de la red.

- Burlar los mecanismos de seguridad, autenticación, autorización o de auditoria de cualquier servicio de red, aplicación, servidor, o cuenta de usuario.

- Interferir o negar el servicio a usuarios autorizados con el propósito de lesionar la prestación del servicio o la imagen de la universidad.

- Uso de comandos o programas o el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

- Proporcionar información sobre los aspirantes, estudiantes, empleados administrativos o docentes a personas o entidades externas que no tengan ningún tipo de relación contractual, relación jurídico-administrativa o convenio con la Universidad donde se especifique que ellos pueden disponer de dicha información.

4.4.6 Gestión de Comunicaciones y Operaciones

La gestión de las comunicaciones y operaciones de la Universidad son esenciales para mantener un adecuado nivel de servicio a los alumnos, docentes e investigadores.
Los procedimientos operacionales y las responsabilidades para mantener accesos adecuados a los sistemas, así como el control y la disponibilidad de los mismos, deben ser incluidos en las funciones operativas de la Universidad.

a) Procedimientos y responsabilidades de operación

- Se deben documentar y mantener los procedimientos de operación identificados por la política de seguridad. Estos procedimientos, se deben tratar como documentos formales y sus cambios han de autorizarse por la dirección.

- Se deben controlar los cambios en los sistemas y recursos de tratamiento de información. Un control inadecuado de dichos cambios es una causa habitual de fallos de seguridad o del sistema. Se deben implantar responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos.

- La separación de los recursos para desarrollo, prueba y producción es importante para conseguir la segregación de las responsabilidades implicadas. Se deberían definir y documentar las reglas para transferir el software del entorno de desarrollo al de producción y así evitar problemas operacionales.

- La contratación de un proveedor externo para gestionar los recursos de tratamiento de información puede introducir posibles vulnerabilidades, como la posibilidad de daño, pérdida o comprometer los datos en las instalaciones de la Universidad. Se deberían identificar estos riesgos de antemano e incorporarse al contrato las medidas de seguridad apropiadas de acuerdo con la Universidad.

b) Gestión de respaldo y recuperación

- Almacenar un nivel mínimo de información de respaldo, junto a los registros exactos y completos de las copias de seguridad y a procedimientos documentados de recuperación, a una distancia suficiente para evitar todo daño por un desastre en el local principal. Se retendrán como mínimo tres generaciones o ciclos de información de respaldo para las aplicaciones importantes del negocio.

- Dar a la información de respaldo un nivel adecuado de protección física y del entorno, un nivel consistente con las normas aplicadas en el local principal. Se deberían extender los controles y medidas aplicados a los medios en el local principal para cubrir el local de respaldo.

- Los medios de respaldo se deben probar regularmente, donde sea factible, para asegurar que son fiables cuando sea preciso su uso en caso de emergencia. Comprobar y probar regularmente los procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación.

c) Protección de software malicioso

- Política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado para los empleados, alumnos, docentes y terceros,
- Verificación de todo archivo adjunto al correo electrónico o de toda descarga para buscar software malicioso antes de usarlo.

- Está prohibido para el personal, el uso de diskettes, discos compactos, memorias USB provenientes de otras fuentes que no sea de la Universidad, a excepción de los provenientes de organismos reguladores, proveedores y clientes, alumnos y docentes, los cuales deben pasar por un procedimiento de verificación y control en el área respectiva.
- Procedimientos y responsabilidades de administración para la utilización de la protección de antivirus, la formación para su uso, la información de los ataques de los virus y la recuperación de éstos
- Se debe evitar compartir archivos o carpetas con otros usuarios; en caso de ser necesario coordinar con el área respectiva y habilitar el acceso sólo a nivel de lectura informando a personal de Soporte Técnico.
- Todos los PCs, laptops y estaciones de trabajo deben tener configurados un protector de pantalla con clave y con un tiempo de espera máximo de 10 minutos o con *logging-off automático cuando el* equipo esté desatendido.

d) Intercambio de información y software

- Los mensajes enviados a listas de correo o grupos de discusión por los miembros de la comunidad universitaria y que utilicen las direcciones de correo de la universidad deben contener un párrafo donde diga "las opiniones *expresadas en este mensaje son estrictamente personales y no es una posición oficial de la Universidad ". Se recomienda que los* mensajes de correo electrónico y las cubiertas (cover) de fax con información confidencial incluyan la siguiente nota:

    - CONFIDENCIAL. UNIVERSIDAD PRIVADA SAN JUAN BAUTISTA

- La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona o la organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenvíelo y borre el mensaje recibido inmediatamente.

- Los miembros de la comunidad universitaria deben ser cuidadosos cuando abran los anexos (attachments) colocados en los mensajes de correo electrónico que sean recibidos de remitentes desconocidos o sospechosos ya que pueden contener virus.
- Está totalmente prohibido lo siguiente :

- ✓ Enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).
- ✓ Generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
- ✓ Envío de mensajes de correo electrónico con una dirección de correo diferente al verdadero remitente con el fin de realizar algún tipo de acoso, difamación u obtener información.
- ✓ Crear o reenviar cartas cadena o cualquier otro tipo esquema de "pirámide" de mensajes
- ✓ Colocar mensajes de correo iguales o similares no relacionados con las actividades de la universidad a un gran número de grupo de noticias (mensajes electrónicos masivos no solicitados y no autorizados en grupos de noticias).

4.4.7 Desarrollo y Mantenimiento de los Sistemas

El diseño de la infraestructura de la Universidad, las aplicaciones de negocio y las aplicaciones del usuario final deben soportar los requerimientos generales de seguridad documentados en la política de seguridad de la Universidad. Estos requerimientos deben ser incorporados en cada paso del ciclo de desarrollo de los sistemas, incluyendo todas las fases de diseño, desarrollo, mantenimiento y producción.

Todos los requisitos de seguridad, incluyendo las disposiciones para contingencias, deberían ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

4.4.8 Cumplimiento Normativo

Se deben cumplir los siguientes objetivos:

- Evitar infringir cualquier norma civil o penal. Ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.

- Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad
- Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoría del proceso.
- Buscar el asesoramiento sobre requisitos legales específicos de los asesores legales de la organización, o de profesionales de derecho calificados.

4.4.9 Gestión de Continuidad del Negocio

El objetivo es reaccionar a la interrupción de las actividades de la Universidad y proteger sus procesos críticos frente a grandes fallos o desastres. Se debe implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallas de seguridad como por ejemplo desastres naturales, accidentes, fallas de equipos o acciones deliberadas mediante una combinación de controles preventivos y de recuperación. Se debe desarrollar e implantar planes de contingencia para asegurar que los procesos de negocio se pueden restaurar en los plazos requeridos, dichos planes se deben mantener y probar para que se integren con todos los demás procesos de gestión.

Proceso de Gestión de la continuidad del negocio

- Comprender los riesgos que la Universidad corre desde el punto de vista de su vulnerabilidad e impacto, incluyendo la identificación y priorización de los procesos críticos del negocio;
- Comprender el impacto que tendrían las interrupciones en las actividades de la Universidad. Es importante encontrar soluciones que manejen las pequeñas incidencias así como los grandes accidentes que puedan amenazar la viabilidad de la organización.
- Tiempo de respuesta lo mínimo posible cuando la Universidad haya sufrido una infracción de seguridad como por ejemplo la infección de virus informáticos en los servidores. Supervisar que los servidores y los firewall marchen bien.
- Probar y actualizar regularmente los planes y procesos que describen las acciones a realizar tras una contingencia que amenace las actividades de la Universidad. Por ejemplo que los procedimientos de las copias de seguridad de la información funcionen adecuadamente.

- Considerar la adquisición de los seguros adecuados que formarán parte de los proceso de continuidad del negocio;
- Formular y documentar planes de continuidad del negocio en línea con la estrategia acordada por la Universidad

4.5 IMPLEMENTACION

Con la identificación de riesgos, amenazas y vulnerabilidades se pudo determinar el conjunto de actividades más importantes a ser realizadas por la Universidad, las cuales permiten alinear las estrategias o medidas de seguridad existentes con las exigidas por las políticas de seguridad elaboradas.

Estas actividades han sido agrupadas en un plan de implementación, el cual contiene las metas de cada actividad, y las etapas a ser cubiertas en cada actividad identificada.

4.5.1 Clasificación de la Información

Metas	Clasificar los activos de información de manera adecuada con el objetivo de priorizar la utilización de recursos para aquella información que requiere de mayores niveles de protección.
Etapas	• Elaboración de un inventario de activos de información incluyendo información almacenada en medios digitales e información impresa. • Definición de responsables por activos identificados • Clasificación de la información por parte de los responsables definidos. • Consolidación de los activos de información clasificados. • Determinación de las medidas de seguridad a ser aplicados para cada activo clasificado. • Implementación de las medidas de seguridad determinadas previamente.

4.5.2 Campaña de concienciación de usuarios

Metas	Lograr un compromiso y concienciación de los miembros de la comunidad universitaria en temas referentes a la seguridad de la información. Se debe realizar una campaña de concienciación que esté orientada a todos los usuarios y relacionada con conceptos básicos de seguridad y a grupos específicos con temas correspondientes a sus responsabilidades en la institución.
Etapas	• Definición del mensaje a transmitir y material a ser empleado para los distintos grupos de usuarios, entre ellos : **Comunidad en general:** Información general sobre seguridad, Políticas de seguridad y estándares incluyendo protección de virus, contraseñas, seguridad física, sanciones, correo electrónico y uso de Internet. **Personal de TIC:** Políticas de seguridad, estándares y controles específicos para la tecnología y aplicaciones utilizadas. **Dirección y Jefaturas:** Monitoreo de seguridad, responsabilidades de supervisión, políticas de sanción. • Capacitación mediante charlas, videos, presentaciones, afiches, etc., los cuales recuerden permanentemente al usuario la importancia de la seguridad de la información.

4.5.3 Seguridad de red y comunicaciones

Metas	Para evitar manipulación de los equipos de comunicaciones por personal no autorizado y garantizar que la configuración que poseen, brinden mayor seguridad y eficiencia a las comunicaciones, se requiere que los equipos que soportan dicho servicio se encuentren adecuadamente configurados.
Etapas	• Adaptación de los equipos y sistemas de comunicaciones a políticas de seguridad.

	• Elaboración de un inventario de equipos de comunicaciones (routers, switches, firewalls, etc.) • Adaptación de los equipos a la política de seguridad • La arquitectura de red propuesta debe considerar la segmentación del área académica como administrativa tanto a nivel hardware como software, • Controlar mediante un firewall la comunicación entre la red de la Universidad y redes externas para evitar actividades no autorizadas desde dichas redes hacia los equipos de red de la Universidad. • Implementar una estructura de la red para evitar el ingreso de conexiones desde Internet hacia la red interna de datos. • Implementar un sistema de Antivirus para servicios de Internet. • Implementar un sistema de monitoreo de Intrusos para detectar los intentos de intrusión o ataque desde redes externas hacia la red de datos de la Universidad. • Implementar un servidor de gestión de seguridad de la red que monitoree todos los demás servidores como antivirus, web, firewall, correo electrónico, etc.

4.5.4 Inventario de accesos a los sistemas

Metas	Con el propósito de obtener un control adecuado sobre el acceso de los usuarios a los sistemas de la Universidad, se debe realizar un inventario de todos los accesos que poseen ellos sobre cada uno de los sistemas. Este inventario debe ser actualizado al modificar el perfil de acceso de algún usuario y será utilizado para realizar revisiones periódicas de los accesos otorgados en los sistemas.
Etapas	• Elaboración de un inventario de las aplicaciones y sistemas de la Universidad. • Elaboración de un inventario de los perfiles de acceso de cada sistema • Verificación de los perfiles definidos en los sistemas para cada

	usuario. • Revisión y aprobación de los accesos por parte de las direcciones respectivas • Depurar los perfiles de accesos de los usuarios a los sistemas • Mantenimiento periódico del inventario.

4.5.5 Adaptación de contratos con proveedores

Metas	Asegurar el cumplimiento de las políticas de seguridad de la Universidad en el servicio brindado por los proveedores, necesario para realizar una revisión de los mismos y su grado de cumplimiento respecto a las políticas de seguridad definidas. Si es necesario dichos contratos deben ser modificados para el cumplimiento de la política de seguridad de la Universidad.
Etapas	• Elaboración de cláusulas estándar referidas a la seguridad de la Información, para ser incluidas en los contratos con proveedores. • Elaboración de un inventario de los contratos existentes con proveedores • Revisión de los contratos y analizar el grado de cumplimiento de la política de seguridad • Negociar con los proveedores para la inclusión de las cláusulas en los contratos.

4.5.6 Verificación y Adaptación de los sistemas de la Universidad

Metas	Para asegurar el cumplimiento de la política de seguridad en los controles existentes, se debe verificar el grado de cumplimiento de las políticas de seguridad en los sistemas de la Universidad y adaptarlos en caso de verificar su incumplimiento.
Etapas	• Elaboración de un inventario de las aplicaciones existentes. • Elaboración de un resumen de los requisitos que deben cumplir las

	aplicaciones según las políticas y estándares de seguridad • Evaluación del grado de cumplimiento de la política de seguridad para cada una de las aplicaciones existentes y la viabilidad de su modificación para cumplir con las políticas de seguridad, elaborando la relación de cambios que deben ser realizados en cada aplicación. • Estandarización de controles para contraseñas de los sistemas.

4.5.7 Revisión y adaptación de procedimientos complementarios

Metas	Adaptar los procedimientos y controles complementarios de la Universidad de acuerdo a lo estipulado en las políticas de seguridad
Etapas	• Revisión y adaptación de los controles y estándares para desarrollo de sistemas. • Elaboración de procedimientos de monitoreo, incluyendo procedimientos para verificación periódica de carpetas compartidas, generación de copias de respaldo de información de usuarios, aplicación de controles de seguridad para información en computadoras portátiles, etc. • Elaboración de procedimientos de monitoreo y reporte sobre la administración de los sistemas y herramientas de seguridad, entre ellas: antivirus, servidores de seguridad del contenido, servidor Proxy, servidor Firewall , sistema de detección de intrusos. • Revisión y establecimiento de controles para el almacenamiento físico de la información • Revisión y establecimiento de controles para personal externo que realiza labores utilizando activos de información de la Universidad para la Universidad. (Soporte técnico, proveedores de comunicación: Telmex, Telefónica, etc.)

4.6 CRONOGRAMA

ACTIVIDAD	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10
Clasificación de Información										
Campaña de concienciación de usuarios										
Seguridad de red y comunicaciones										
Inventario de accesos a los sistemas										
Adaptación de contratos con proveedores										
Verificación y adaptación de los sistemas de la Universidad										
Revisión y adaptación de procedimientos complementarios										

4.7 EVALUACION DE LAS ESTRATEGIAS DE SEGURIDAD

Estrategias o medidas de seguridad	Indicadores De Gestión
• Estándares de seguridad para servidores con sistemas operativos Windows y Linux • Revisiones periódicas de los registros de los sistemas y operaciones realizadas por los usuarios • Restricciones en el manejo de la información enviada por correo electrónico hacia redes externas	• Incremento de los niveles de seguridad de la información a los servidores de base de datos y servidores de aplicaciones. • Reducción de abusos de Internet por parte de los usuarios • Tasa de incidencias de seguridad ocasionada por intrusos internos como externos.
• Adecuada arquitectura e implementación del sistema antivirus • Verificación periódica de la actualización del antivirus de computadoras personales y servidores. • Generación periódica de reporte de virus detectados y actualización de Antivirus.	• Reducción de archivos infectados por virus informáticos • Incremento de la productividad en la institución
• Uniformizar dentro de lo posible la estructura de las contraseñas empleadas y sus fechas de renovación • Implementar un sistema de Servicio de Directorio, el cual permita al usuario identificarse en él, y mediante un proceso automático, éste lo identifique en los sistemas en los cuales posee acceso.	• Incremento de los niveles de seguridad de la información. • Reducción general del tiempo de ciclo de reestablecer contraseñas cada vez que el usuario se olvida.

• Programa de capacitación de la Universidad en temas relacionados a la seguridad de la información.	• Grado de compromiso y responsabilidad con el manejo de la información • Comparar el número de incidencias de seguridad por parte de los usuarios en períodos diferentes.
• Diseño de arquitectura de seguridad de red • Adecuada configuración de elementos de control de conexiones (Firewalls) • Implementación y administración de herramientas de seguridad • Separación del segmento de red inalámbrico mediante un firewall.	• Tasa de incidencias de seguridad ocasionada por intrusos internos como externos. • Reducción de los riesgos de la información
• Establecimiento de un procedimiento formal que contemple la generación de copia de respaldo de información importante de los usuarios. • Asegurar que la información del usuario que se almacene en el servidor esté protegida por una contraseña.	• Incremento de confiabilidad y productividad de por parte de los usuarios • Adecuado respaldo de la información.
• Implementación y administración de herramientas para la inspección del contenido de los correos electrónicos	• Reducción de abusos de mensaje de correo electrónico no solicitado ni autorizado dentro de la institución.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1. La seguridad de la información ha sido siempre considerada como un problema de ingeniería, donde la responsabilidad debe recaer en el personal de Tecnología de Información y Comunicaciones, de tal forma que las organizaciones han tratado de resolverlo utilizando tecnología como controles de acceso pero este enfoque es incorrecto porque la gestión de la seguridad de la información requiere la participación de todos los empleados de una organización. Los resultados de la investigación demuestran que la estrategia de desarrollar políticas de seguridad de la información es de prioridad en las Universidades: UNMSM 37%, UNFV 19% y UPSJB 24%.

2. Las autoridades no consideran a la seguridad como una prioridad alineada con la estrategia universitaria. Ello se refleja en las encuestas realizadas al personal de TIC donde se les formuló la pregunta si habían asistido a eventos o programas de capacitación de seguridad de la información, la cual reportó que la mayoría nunca asistió a programas de capacitación: UNMSM 20%, UNFV 100% y UPSJB 70%. De tal manera que la estrategia de capacitación es de mucho interés por el personal: UNMSM el 60%, UNFV el 70% y UPSJB el 70%.

3. Los resultados de la investigación con respecto a los riesgos de la información en las Universidades como son: la divulgación ilícita de la información por los trabajadores (UNFV 36%), no realizar copias de seguridad (UPSJB 28%), virus informáticos (UNMSM 56%), corroboran con lo que está pasando a nivel mundial, donde el 70% de los robos o accidentes que se producen en los sistemas informáticos de las organizaciones los causan los propios trabajadores, muchas veces son resultados de errores, descuidos en sus conocimientos sobre la seguridad de la organización o actos delictivos propiamente dichos.

4. A diferencia de las redes informáticas corporativas y otras redes comerciales, que son más cerradas y segmentadas con énfasis en la protección de los recursos valiosos de la información, las redes universitarias están diseñadas para funcionar como proveedores del servicio de Internet, facilitar el acceso a los usuarios y facilitar el flujo de la información. En la presente investigación, los resultados revelan que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en

la seguridad: UNMSM 70%, UNFV 62% y UPSJB el 70%. Las razones principales sobre estos resultados fueron que en la Universidad como centro de investigación no debe haber restricciones al acceso de la información. Otra razón fue que cuando fueron diseñadas las redes universitarias no había Internet o recién estaba apareciendo, y por tanto no había demasiados riesgos a la información desde el exterior de la institución.

5. En una organización existen recursos humanos, recursos técnicos e infraestructura que están expuestos a diferentes tipos de riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, virus informáticos, espionajes, sabotaje, vandalismo y otros. La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas de seguridad, y se han vuelto más vulnerables al compartir sus recursos de información e interconectar las redes públicas (Internet) con las privadas. Los hackers pueden penetrar a las redes informáticas de una institución y causar graves interrupciones en el sistema.

6. La seguridad de la información está siendo un tema crítico dentro de las organizaciones, y por tanto deben establecerse requisitos de seguridad en la parte legal como normativas, estatutos, regulaciones y contratos que deberían satisfacer las organizaciones, los contratistas y los proveedores de servicios, de tal forma que se garantice la seguridad de los activos, la exactitud y confiabilidad de sus registros y la aceptación de las normas administrativas.

5.2 RECOMENDACIONES

1. Muchos sistemas de información no han sido diseñados para ser seguros, y la seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. Las universidades deben implementar políticas de seguridad de la información o hacerlas cumplir si las tienen, pues son la base para la gestión de seguridad. La implementación de las estrategias o medidas de seguridad, para que sea eficaz, debe basarse en un plan organizado que tenga en cuenta todos los aspectos de las necesidades de seguridad de la organización.

2. Se deben implementar programas de capacitación de seguridad de la información en la universidad comenzando por la cima de la escala jerárquica; primero implementar el programa de seguridad para las autoridades, los jefes de departamentos, luego trabajadores, estudiantes, docentes y personal externo que brinda servicios.

3. Muchas organizaciones tienen políticas de seguridad, pero muy pocas implantan una cultura de conciencia de seguridad que fomente la identificación del trabajador con la información que manejan. Para que tenga éxito un plan de gestión de seguridad en las Universidades es necesario un marketing efectivo de seguridad de la información a las autoridades universitarias, docentes, alumnos, trabajadores y terceros. Debe haber normas y guías que controlen la forma en la que se lleva a cabo el plan, y que se distribuya en forma de políticas.

4. A la luz de las recientes brechas de seguridad y de las expectativas de más amenazas a la seguridad en el futuro, las Universidades no pueden continuar con un acceso abierto e ilimitado de la información. Se deben rediseñar las redes informáticas de las universidades separando el área académica y el área administrativa pues tienen sistemas administrativos críticos. Es necesario consolidar sus redes informáticas aplicando tecnología de prevención y detección de intrusos, que es una buena solución para observar el tráfico de la red, permitir el ingreso del tráfico legítimo y detectar comportamientos maliciosos como los ataques de negación de servicios para evitar interrupciones en la red.

5. Para minimizar los efectos de un problema de seguridad se realiza lo que llamamos un análisis de riesgos y responder a tres cuestiones básicas sobre nuestra seguridad:

- ¿Qué queremos proteger?
- ¿Contra quién o qué lo queremos proteger?
- ¿Cómo lo queremos proteger?

Debemos planificar no sólo la prevención ante un problema sino también la recuperación si el mismo se produce, y recuperarnos de ese incidente en el menor tiempo posible y el menor costo, por ello es necesario que las instituciones cuenten con un plan de continuidad del negocio cuando se han producido desastres o fallas de seguridad.

6. Existen estándares internacionales sobre seguridad de la información. Las más conocidas son la ISO 17799 que es una compilación de recomendaciones para las buenas prácticas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector, y la ISO 27001 que es un sistema de gestión de seguridad de la información que comprende los procedimientos adecuados y la planificación e implantación de controles de seguridad basadas en una evaluación de riesgos. En el País, la Presidencia del Consejo de Ministros (PCM) a través de la Oficina Nacional de Gobierno Electrónico, dispone del uso obligatorio de la Norma Técnica Peruana ISO 17799:2004 para ser implementada en Entidades Públicas. Esta norma se ha basado en la norma internacional ISO/IEC 17799:2000.

BIBLIOGRAFIA

ACEITUNO, Vicente. *Definición de seguridad de la información y sus limitaciones*. [En línea] http://www.fistconference.org/data/presentaciones/queesseguridad.pdf. [Consulta :08 Mayo de 2006]

ASENSIO, Gonzalo*. Seguridad en Internet*. Ediciones Nowtilus S.L. 2006

CALLE GUGLIERI, José A. Reingeniería y Seguridad en el Ciberespacio. Díaz de Santos. Madrid. 1996.

CHIAVENATO, Idalberto. *Introducción a la teoría general de la administración.* S´ptima Edición. McGRAW-HILL. México. 2006.

CORDOVA RODRIGUEZ, Norma*. Plan de seguridad informática para una entidad financiera*. [En línea] http://sisbib.unmsm.edu.pe/bibvirtual/Tesis/Basic/cordova_rn/cordova_rn.htm. [Consultado: 05 de Agosto de 2006]

DOMINGO, Gonzalo Ernesto. *Seguridad en las transacciones on line de comercio electrónico*. [En línea] http://www.eiidi.com/Download/**Seguridad**%20de%20**transacciones**%20en%20**linea**.pdf [Consultado: 15 de Diciembre de 2006]

DRUKER, F. Peter. *Los desafíos de la Gerencia para el siglo XX!*. Norma. Bogotá. 1999.

ENCICLOPEDIA WIKIPEDIA. [En línea] http://es.wikipedia.org/wiki/Universidad [Consulta: 10 de Enero de 2007]

ESPINOZA HERRERA, Nemesio. *Gerencia Universitaria. Universidad Peruana y Tercer Milenio*. Editorial "San Marcos", 2000.

EL PORTAL DE ISO 27000 EN ESPAÑOL. [En línea] http://www.iso27000.es/iso27000.html. [Consulta: 12 de Enero de 2007]

GASPAR, Juan. *Planes de Contingencia*. Díaz de Santos. Madrid. 2004

JOSHI, James B.D. y Otros. "Security Models for Web-Based Applications". Communications of the ACM 41, núm. 2 Febrero de 2001.

KOONTZ, Harold y Heinz Weihrich. *Administración. Una perspectiva global.* Décima Edición. McGRAW-HILL. México. 2004.

LAUDON Kennet C. y Jane P. LAUDON. *Sistemas de Información Gerencial*. Octava edición, Pearson Educación de México. 2004.

MCLEOD Jr., Raymond. *Sistemas de información gerencial*. Séptima Edición Prentice May Hispanoamericana. México. 2000.

MOLINA MATEOS, José María. *Criptología y Derecho. Colección Seguridad de la Información y Derecho*. El Cid Editor. Madrid. 2000.

MOLINA MATEOS, José María. *Seguridad de la información*. *Criptología*. El Cid Editor. Madrid. 2000.

OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA. *Primera Encuesta Nacional de Seguridad de la Información en la Administración Pública-2004* [En línea] www.pcm.gob.pe/portal_ongei/publicaciones/I**Encuesta**de**Seguridad**.pdf. [Consulta: 10 de Octubre de 2006]

OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA. *Norma Técnica Peruana ISO/17799 2004. Tecnología de la información. Código de Buenas prácticas para la gestión de la seguridad de la información*. [En línea] www.ongei.gob.pe/bancos/banco_normas/archivos/P01-PCM-ISO17799-001-V1.pdf . [Consulta: 10 de Octubre de 2006]

OPPLIGER, Rolf. "Internet Security. Firewalls and Beyond". Communications of de ACM 41, núm.7 Mayo de 1997.

PEREZ AGUDIN, Justo y Otros. *La Biblia del Hacker*. Anaya Multimedia. Madrid. 2006.

PESO NAVARRO, Emilio del. *Servicios de la sociedad de la información.* Díaz de Santos. Madrid 2003. 387 págs.

PESO NAVARRO, Emilio del y Miguel Ángel **RAMOS GONZALEZ**. *La seguridad de los datos de carácter personal*. Díaz de Santos. Madrid. 2002.

PESO NAVARRO, Emilio del. *Manual de Outsourcing Informático*. Díaz de Santos. Madrid, 2003.

PESO NAVARRO, Emilio del. *El Documento de Seguridad* .Díaz de Santos. Madrid. 2004.

RAINER, Rex Kelley y Otros. "Risk Analysis for Information Technology". Journal of Management Information Systems 8, núm. 1. 1991.

RIBAGORDA GARNACHO, Arturo. "La auditoría de las redes de ordenadores". Documentación. Conferencia AUDISI'2000. IEE

RODRIGUEZ LOPEZ, Margarita. *La influencia de la cultura organizacional en la implantación de la estrategia de seguridad de la información en una organización financiera*. [En línea] http://www.bib.uia.mx/tesis/pdf/014510/014510.pdf.[Consultado: 10 de Diciembre de 2006]

RODRIGUEZ HERNANDEZ, Eduardo. *Arquitectura de Seguridad de la Red Inalámbrica Universitaria*. [En línea]. http://www.astralix.com/papers/riu-titulacion-espina.pdf [Consultado: 12 de Octubre de 2006]

RODRIGUEZ VALENCIA, Joaquín. *Administración I.* Thomson Learning Ibero. 2006.

SEGEV, Arie y Otros. "Internet Security and the Case of Bank of America". Communications of the ACM 41, núm. 10. Octubre de 1998.

SHINDER, Debra Littlejhon. Prevención y Detección de delitos informáticos. Ed. Anaya Multimedia, Madrid. 2003.

SCHMITZ, Oscar. *Principios básicos de seguridad de la información* [En línea] http://conosur.cio.com/blogs/node/16 [Consulta: 15 de Enero de 2007]

STONER, James y Edward Freeman. *Administración.* Sexta Edicion. Prentice-Hall-Hispanoamericana,S.A. México. 1996

STRAUB, Detmar y **WELKE**, Richard. "Coping with Systems Risk: Security Planning Models for Management decision Making", MIS Quarterly 22 núm4. Diciembre de1998.

SYMANTEC CORPORATION. "Universidades abordan el problema del robo de identidad". [En línea]: http://www.symantec.com/region/mx/enterprisesecurity/content/government/LAM_3583.html [Consulta: 15 Mayo de 2006]

TELEFÓNICA DEL PERÚ. Empresas en linea. [En línea] http://www.telefonica.com.pe/empresas/boletines/pdf/bolemprejulio06.pdf. [Consulta: 10 de Enero de 2007]

UNIVERSIDAD CARLOS III de MADRID. La innovación al servicio del alumno. Año 2005. [En línea] http://www.microsoft.com/spain/enterprise/casestudies/cs_uni_carlosiii01.aspx

WEBER, Ron. *Information Systems Control and audit*. Prentice Hall. New York. 1998.

ANEXOS

Anexo Nº 1

Encuesta de opinión a expertos en Tecnología de Información y Comunicaciones

Sr. /Sra. Estamos realizando encuestas a expertos de TIC en forma anónima, para una Tesis de Maestría. Por ello, mucho agradeceré se sirva absolver tales preguntas. MUCHAS GRACIAS

1. ¿En la Universidad donde labora tienen políticas de seguridad de la información?

[ ] Si
[ ] No

2. ¿Si en la Pregunta 1 respondió si, Se cumplen o se llevan a la práctica estas políticas?

[ ] A cabalidad
[ ] Medianamente
[ ] No se cumplen

3.Elija los beneficios que se presentan cuando la Universidad cuenta con políticas de seguridad de la información. Marcar uno o más opciones.

[ ] Mayor seguridad de la información mediante el respaldo de medios magnéticos
[ ] Aumenta la productividad a través de consultas directas y confiables
[ ] Calidad en el servicio para los alumnos, docentes y terceros
[ ] Otros
……

4.¿Cuáles de estas medidas de seguridad de la información son más importantes para Usted?. Marcar uno o más opciones.

[ ] Desarrollo de Políticas de Seguridad
[ ] Clasificación del acceso de la información
[ ] Capacitación de usuarios
[ ] Monitoreo y reportes de las actividades en la red informática
[ ] La continuidad del negocio después de ataques de intrusos
[ ] Otros
……

5. ¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico?. Marcar uno o más opciones.

[ ] Omitir la seguridad como un aspecto fundamental de configuración del servidor
[ ] Transmisión en pleno texto de contraseñas
[ ] Uso inadecuado de herramientas de seguridad, o no uso alguno
[ ] Obtener y mantener programas y aplicaciones (software) que son vulnerables
[ ] No tomar medidas preventivas en los aspectos de seguridad relevantes
[ ] Otros
……

6. ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información ?. Marcar en el cuadro todos los riesgos y frecuencias presentados.
MF: Muy frecuente RF: Regularmente frecuente PF: Poco frecuente

RIESGOS	MF	RF	PF
Fenómenos Naturales (Terremotos, Inundaciones)			
Fallas mecánicas (Cortes de fluido eléctrico, incendios)			
Divulgación ilícita de la información por el personal			
Destrucción o modificación de la información por el personal			
Intrusos al sistema de la red			
Virus informáticos, gusanos, spam			
Otros:			

7. ¿Sus equipos de cómputo en su área tienen fuente de poder ininterrumpible (UPS), generadores de energía, baterías ante cortes de energía eléctrica?

[ ] Si
[ ] No

8, ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

[ ] Saturación de la red por programas indebidos (música, video)
[ ] Uso del correo electrónico de la Universidad para fines personales
[ ] Pérdida de su información
[ ] Olvido de contraseña
[ ] No realizar copias de seguridad
[ ] Accesar a carpetas compartidas de otros usuarios
[ ] Otros
……

9. ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

[ ] Hace 3 meses
[ ] Hace 6 meses
[ ] Hace 1 año
[ ] Nunca

10. ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

[ ] Muy interesado
[ ] Poco interesado
[ ] Nada interesado

11. ¿Considera que la mayoría de las redes informáticas universitarias fueron diseñadas sin pensar originalmente en la seguridad?

[ ] Si
[ ] No

Porqué?
……
……..

12. ¿Cómo considera la gestión de seguridad de la información en la gestión académica y administrativa de la Universidad sobre los sistemas de información como son: matrícula de alumnos, admisión y registros, tesorería, y trámites documentarios?
[ ] Buena
[ ] Regular
[ ] Mala

13. ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la Universidad?

[ ] Muy beneficioso
[ ] Poco beneficioso
[ ] Nada beneficioso

Anexo Nº 2

RESOLUCION MINISTERIAL N° 310-2004-PCM

Lima, 4 de Octubre de 2004

CONSIDERANDO:

Que, el artículo 2° del Decreto Supremo N° 066-2003-PCM y el numeral 3.10 del artículo 3° y artículo 22° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 067-2003-PCM, prevén que la Presidencia del Consejo de Ministros se encarga de normar, coordinar, integrar y promover el desarrollo de la actividad informática en la Administración Pública, impulsando y fomentando el uso de las nuevas tecnologías de la información para la modernización y desarrollo del Estado, actúa como ente rector del Sistema Nacional de Informática, dirige y supervisa la política nacional de informática y gobierno electrónico;

Que, de acuerdo con los numerales 25.2 y 25.3 del artículo 25° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 067- 2003-PCM, son funciones de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros, proponer la normatividad y coordinar el desarrollo del gobierno electrónico y de la actividad informática en la Administración Pública, impulsando su modernización, y desarrollar acciones orientadas a la consolidación y desarrollo del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial N° 224-2004-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. 1ª Edición" en las entidades integrantes del Sistema Nacional de Informática;

Que, la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros - ONGEI ha propuesto ejecutar la Primera Encuesta de Seguridad de la Información en la Administración Pública - 2004, para obtener y mantener actualizada la información técnica relacionada con la seguridad de la información de las instituciones del Sistema Nacional de Informática;

De conformidad con lo dispuesto por el Decreto Legislativo Nº 560 - Ley del Poder Ejecutivo y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo Nº 067-2003-PCM;

SE RESUELVE:

Artículo 1º.- Autorizar la ejecución de la "Primera Encuesta de Seguridad de la Información en la Administración Pública - 2004" en todas las instituciones públicas pertenecientes al Sistema Nacional de Informática.

Artículo 2º.- La ejecución y la actualización de la Encuesta de Seguridad de la Información en la Administración Pública" será efectuada por la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros.

Artículo 3º.- Las instituciones públicas deberán remitir documento de la encuesta a la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros hasta el 15 de diciembre del 2004, de acuerdo a las indicaciones y a la información solicitada en el anexo adjunto, que constituye parte integrante de la presente Resolución Ministerial.

Regístrese, comuníquese y publíquese.

CARLOS FERRERO
Presidente del Consejo de Ministros

F*uente:* Publicada en el Diario Oficial El Peruano el 06/10/2004.

Anexo Nº 3

ISO 27001: Sistema de Gestión de la Seguridad de la Información

SGSI es la abreviatura comúnmente utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS son las siglas equivalentes en el idioma inglés y en relación a *Information Security Management System*.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad de la seguridad de la información.

Importancia de un SGSI

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que pueden aprovechar cualquiera de las vulnerabilidades existentes en la organización para someter activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el “hacking” o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos por su elevado nivel de sofisticación, pero también se deben considerar los riesgos a sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización. El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio son algunos de los aspectos fundamentales en los que un SGSI significa una herramienta definitiva para su consecución en las organizaciones y de importante ayuda para la gestión de las mismas.

El nivel de seguridad alcanzado por medios técnicos demuestra ser invariablemente limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización con la dirección al frente y se debe considerar, adicionalmente, a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la

planificación e implantación de controles de seguridad basadas en una evaluación de riesgos y una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos propios y de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y actualiza constantemente.

¿Qué incluye un SGSI?

Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles como se puede aprecia en la figura Nº 2.

Figura Nº 2
Documentos del SGSI

F*uente:* www.iso27000.es

La documentación debe incluir los registros de las decisiones de la dirección, asegurar que se puedan seguir los indicios de las decisiones de la dirección y las políticas, así como permitir que los resultados registrados sean reproducibles.

¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad:

- ***Plan (planificar):*** establecer el SGSI.
- ***Do (hacer):*** implementar y utilizar el SGSI.
- ***Check (verificar):*** monitorizar y revisar el SGSI.
- ***Act (actuar):*** mantener y mejorar el SGSI.

A continuación detallamos cada uno de ellos:

***Plan:* Establecer el SGSI**

Definir alcance del SGSI: según el modelo organizativo, definir los límites del marco de dirección de seguridad de la información.

- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización.
- Inventario de activos: todos aquellos afectados por la seguridad de la información.
- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Análisis de riesgos: evaluar el daño resultante de un fallo de seguridad y la probabilidad de ocurrencia del fallo.
- Selección de controles.
- Definir plan de tratamiento de riesgos: que identifique las acciones, sus responsables y las prioridades en la gestión de los riesgos de seguridad de la información.

Do: **Implementar y utilizar el SGSI**

- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se determinaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar todos los recursos asignados al SGSI.

Check : **Monitorizar y revisar el SGSI**

- Revisar el SGSI: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, identificar nuevas vulnerabilidades, revisar cambios organizativos y modificar procedimientos.
- Realizar auditorías internas del SGSI: para determinar la efectividad del SGSI y detectar posibles no conformidades

Act: **Mejora Contínua**

- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades

Anexo Nº 4

Glosario de términos

Con el propósito de unificar significados de algunos términos utilizados en la presente investigación, a continuación se definen las siguientes:

- **Activos:** recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

- **Amenazas:** eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

- **Contraseña:** Una contraseña es un código o una palabra que se utiliza para acceder a datos restringidos de una computadora. Mientras que las contraseñas crean una seguridad contra los usuarios no autorizados, el sistema de seguridad sólo puede confirmar que la contraseña es válida si el usuario está autorizado a disponer de la información.

- **Criptografía :** Es la rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas. Este procedimiento permite la transmisión de informaciones privadas por las redes públicas desordenándola matemáticamente (encriptándola) de manera que sea ilegible para cualquiera excepto para la persona que posea la “llave” que pueda ordenar (desencriptar) la información nuevamente.

- **Detección de Intrusos :** Sistemas utilizados para detectar las intrusiones o los intentos de intrusión; cualquier mecanismo de seguridad con este propósito puede ser considerado sistema de detección de intrusos, pero generalmente sólo se aplica esta denominación a los sistemas automáticos.

- **Dirección IP:** Una dirección IP es un código numérico que identifica a una computadora específica en una red de área local o Internet.

- **Eficacia :** Consecución de los objetivos; logro de los efectos deseados.

- **Eficiencia:** Logro de los fines con la menor cantidad de recursos; el logro de los objetivos al menor costo u otras consecuencias no deseadas.

- **Firewalls:** Una combinación de hardware y software que proporciona un sistema de seguridad, usualmente para ayudar a evitar el acceso de externos no autorizados a una red interna o Intranet.

- **Gestión:** Es el proceso mediante el cual se obtiene, despliega o utiliza una variedad de recursos básicos para apoyar los objetivos de la organización.

- **Hacker:** Persona que obtiene acceso no autorizado a una red de computación para obtener provecho, realizar actos delictivos o por placer personal.

- **Información:** La información es el resultado de haber organizado o analizado los datos de alguna manera y con un propósito.

- **Intrusión:** Se denomina intrusión a un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad; además una intrusión no tiene porque consistir solo en un acceso no autorizado a una máquina, también puede ser una negación de servicio, es decir dejar sin funcionamiento al sistema informático.

- **Mecanismo de Salvaguarda:** procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

- **Política de seguridad de la información:** Una política de seguridad de la información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

- **Permisos :** Regla asociada con un objeto, como un archivo, para regular qué usuarios pueden obtener acceso al objeto y de qué manera. El dueño del objeto otorga o niega los permisos.

- **Riesgo:** posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización

- **Redes informáticas:** Están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información.

- **Red inalámbrica:** una red inalámbrica posibilita la unión de dos o más dispositivos sin la medición de cables. Es una red en la cual los medios de comunicación entre sus componentes son ondas electromagnéticas.

- **Seguridad:** Es la protección de los activos frente acciones o situaciones no deseadas mediante la implantación de controles.

- **Sistema de información :** Se puede definir como un conjunto de componentes interrelacionados que reúne, procesa, almacena y distribuye información para apoyar la toma de decisiones y el control de la organización.

- **Servicios críticos universitarios :** Son los servicios de redes, sistemas y comunicaciones y de apoyo que brinda la Universidad y que manejan información muy valiosa como los datos financieros y presupuestal, registros de historias clínicas de los estudiantes y cuerpo docente, documentos oficiales del Rectorado y Decanatos, documentación de Grados y Títulos, notas de los alumnos, certificados de estudios, etc.

- **Software Antivirus:** Es el software diseñado específicamente para la detección, eliminación y prevención de virus informáticos.

- **Sistema Operativo:** Un sistema operativo (SO) es un conjunto de programas software que permite comunicar al usuario con una computadora y gestionar sus

recursos de manera cómoda y eficiente. Comienza a trabajar cuando se enciende el ordenador, y gestiona el hardware de la máquina desde los niveles más básicos. Hoy en día un sistema operativo se encuentra normalmente en ordenadores o productos electrónicos como teléfonos móviles.

- **Tecnologías de la Información y Comunicaciones (TIC) :** Es un término que se utiliza actualmente para hacer referencia a una gama amplia de servicios, aplicaciones, y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones.
- **Usuario:** Persona que accede a los recursos y servicios que ofrece una red informática. Puede ser un trabajador, docente, alumno o tercero.

- **Virus informático :** Un virus informático es un programa creado especialmente para invadir computadores y redes y crear el caos. El daño puede ser mínimo, como hacer aparecer una imagen o un mensaje en la pantalla, o puede hacer mucho daño alterando o incluso destruyendo archivos dentro de la computadora.